GuardLogix Controller Systems

Allen-Bradley

Catalog Numbers 1756-L61S, 1756-L62S, 1756-L63S, 1768-L43S, 1768-L45S

Safety Reference Manual

Important User Information

Solid state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication SGI-1.1 available from your local Rockwell Automation sales office or online at http://www.rockwellautomation.com/literature/) describes some important differences between solid state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING	Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.
ATTENTION	Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence
SHOCK HAZARD	Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
BURN HAZARD	Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

Rockwell Automation, Allen-Bradley, TechConnect, ControlLogix, GuardLogix, CompactLogix, CompactBlock Guard I/O, ArmorBlock Guard I/O, Guard I/O, ControlFlash, Logix5000, SLC, RSLogix 5000, RSNetWorx for EtherNet/IP, RSNetWorx for DeviceNet, RSNetWorx for ControlNet, FactoryTalk Security, and RSLinx are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

The information below summarizes the changes to this manual since the last publication.

To help you find new and updated information in this release of the manual, we have included change bars as shown to the right of this paragraph.

This manual now covers 1768 Compact GuardLogix controllers as well as 1756 GuardLogix controllers. When 'GuardLogix' is used alone throughout the manual, it refers to both 1756 and 1768 GuardLogix controllers.

Topic	Page
1768 Compact GuardLogix Controller User Manual and Installation Instructions added to list of Additional Resources	11
1768-L43S and 1768-L45S Compact GuardLogix controllers and 1768 power supplies added to list of GuardLogix System Components	16
1784-CF64 and 1784-CF128 CompactFlash cards added to list of GuardLogix System Components	16
1734-AENT POINT I/O Ethernet Adapter added to list of components suitable for use with a GuardLogix system	17
1768-L43S and 1768-L45S Compact GuardLogix controller hardware	25
Information on EN50156 Compliance with 1756 ControlLogix SIL 2 Inputs	45
Storing and Loading a Project from Nonvolatile Memory	62
Using Safety Add-On Instructions	83
PFD and PFH data for 1768-L43S and 1768-L45S controllers	101 and 102
PFD data for 20-year proof test intervals	102
Updated terminology to distinguish between safety task signature, instruction signature, safety instruction signatures	throughout

Preface

Introduction 9
About This Publication 9
Who Should Use This Publication 9
Understanding Terminology 10
Additional Resources 11

Chapter 1

Safety Integrity Level (SIL) Concept

Introduction 13
SIL 3 Certification 13
Functional Verification Tests 14
GuardLogix Architecture for SIL 3 Applications 15
GuardLogix System Components 16
GuardLogix Certifications 18
GuardLogix PFD and PFH Specifications 19
Safety Integrity Level (SIL) Compliance Distribution and Weight 20
System Reaction Time 21
Safety Task Reaction Time 21
Safety Task Period and Safety Task Watchdog 21
Contact Information If Device Failure Occurs 22

Chapter 2

GuardLogix Controller System

Introduction 23
1756 GuardLogix Controller Hardware 23
Primary Controller 24
Safety Partner 24
Chassis 24
Power Supplies 24
1768 Compact GuardLogix Controller Hardware 25
CIP Safety Protocol 25
Safety I/O 25
Communication Bridges 26
Programming Overview 28

Chapter 3

CIP Safety I/O for the GuardLogix Control System

Introduction 29
Overview 29
Typical Safety Functions of CIP Safety I/O Modules 29
Diagnostics 30
Status Data 30
Status Indicators 30
On- or Off-delay Function 30
Reaction Time 31

Safety Considerations for CIP Safety I/O Modules 31
Ownership 31
Safety I/O Configuration Signature 31
I/O Module Replacement 32

Chapter 4

CIP Safety and the Safety Network Number

Introduction 35
The Routable CIP Safety Control System. 35
Unique Node Reference 36
Safety Network Number 36
Considerations for Assigning the Safety Network Number (SNN) 38
Safety Network Number (SNN) for Safety Consumed Tags 38
Safety Network Number (SNN) for Out-of-box Modules. . 38
Safety Network Number (SNN) for Safety Module with a Different Configuration Owner 38
Safety Network Number (SNN) when Copying a Safety Project. 39

Chapter 5

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Introduction 41
Differentiate Between Standard and Safety 41
SIL 2 Safety Applications 42
SIL 2 Safety Control in the Safety Task 42
SIL 2 Safety Control in Standard Tasks (1756 GuardLogix Controllers Only) 45
EN50156 Compliance With 1756 ControlLogix SIL 2 Safety Inputs in Dual-channel Configurations with 1756 GuardLogix Controllers. 45
SIL3 Safety – the Safety Task 47
Safety Task Limitations 48
Safety Task Execution Details 48
Safety Programs 49
Safety Routines 50
Safety Tags 50
Standard Tags in Safety Routines (Tag Mapping) 51
Additional Resources 52

Chapter 6

Safety Application Development

Introduction 53
Safety Concept Assumptions 53
Basics of Application Development and Testing 53
Commissioning Life Cycle 54
Specification of the Control Function 55

Create the Project. 56
Test the Application Program 56
Generate the Safety Task Signature 57
Project Verification Test 57
Confirm the Project 58
Safety Validation 60
Lock the GuardLogix Controller 60
Downloading the Safety Application Program. 61
Uploading the Safety Application Program 61
Online Editing 61
Storing and Loading a Project from Nonvolatile Memory. . . . 62
Force Data 62
Inhibit a Module 63
Editing Your Safety Application 63
Performing Offline Edits 64
Performing Online Edits 64
Edit Your Project 65

Chapter 7

Monitor Status and Handle Faults

Introduction 67
Monitoring System Status. 67
CONNECTION_STATUS Data 67
Input and Output Line Conditioning 68
I/O Module Connection Status 68
De-energize to Trip System 69
Use Connection Status Data to Initiate a Fault Via Program Logic 69
Get System Value (GSV) and Set System Value (SSV) Instructions 74
GuardLogix System Faults 74
Nonrecoverable Controller Faults 75
Nonrecoverable Safety Faults 75
Recoverable Faults 76

Appendix A

Safety Instructions

Introduction 77
Safety Application Instructions 77
Metal Form Safety Application Instructions 79
Safety Instructions 80
Additional Resources 81

Appendix B

Safety Add-On Instructions

Introduction 83
Creating and Using a Safety Add-On Instruction 83
Create Add-On Instruction Test Project 85

Create a Safety Add-On Instruction 85
Generate Instruction Signature 85
Download and Generate Safety Instruction Signature. . . . 86
SIL 3 Add-On Instruction Qualification Test. 86
Confirm the Project 86
Safety Validate Add-On Instructions 87
Create Signature History Entry 87
Export and Import the Safety Add-On Instruction 87
Verify Safety Add-On Instruction Signatures 88
Test the Application Program 88
Project Verification Test 88
Safety Validate Project 88
Additional Resources. 88

Appendix C

Reaction Times

Introduction 89
System Reaction Time 89
Logix System Reaction Time 89
Simple Input-logic-output Chain 90
Logic Chain Using Produced/Consumed Safety Tags 91
Factors Affecting Logix Reaction-time Components 92
Additional Resources 93

Appendix D

Checklists for GuardLogix Safety Applications

Introduction 95
Checklist for GuardLogix Controller System 96
Checklist for Safety Inputs 97
Checklist for Safety Outputs. 98
Checklist for Developing a Safety Application Program. 99

Appendix E

Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH) Data

Introduction 101
GuardLogix Controller and Guard I/O Safety Data 101
PFD Values. 102
PFH Values. 102

Glossary

Index

Introduction

Topic	Page
About This Publication	9
Who Should Use This Publication	9
Understanding Terminology	10
Additional Resources	11

About This Publication

This manual is intended to describe the GuardLogix controller system, which is **type-approved** and certified for use in safety applications up to and including SIL 3 according to IEC 61508 and IEC 62061, safety applications up to and including Performance Level PLe (Category 4) according to ISO 13849-1.

This publication covers both 1756 and 1768 GuardLogix controller systems. When 'GuardLogix controllers' is used alone in this publication, it refers to both 1756 and 1768 GuardLogix controllers. Information specific to one controller type will include the bulletin number, 1756 or 1768.

Who Should Use This Publication

Use this manual if you are responsible for the development, operation, or maintenance of a GuardLogix controller-based safety system. You must read and understand the safety concepts and requirements presented in this manual prior to operating a GuardLogix controller-based safety system.

Understanding Terminology

The following table defines terms used in this manual.

Terms and Definitions

Abbreviation	Full Term	Definition
1oo2	One out of Two	Identifies the programmable electronic controller architecture.
CIP	Common Industrial Protocol	A communication protocol designed for industrial automation applications.
CIP Safety	Common Industrial Protocol – Safety Certified	SIL 3 rated version of CIP
DC	Diagnostic Coverage	The ratio of the detected failure rate to the total failure rate.
EN	European Norm.	The official European Standard.
GSV	Get System Value	A ladder logic instruction that retrieves specified controller status information and places it in a destination tag.
PC	Personal Computer	Computer used to interface with, and control, a Logix-based system via RSLogix 5000 programming software.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
PL	Performance Level	ISO 13849-1 safety rating
SNN	Safety Network Number	A unique number that identifies a section of a safety network.
SSV	Set System Value	A ladder logic instruction that sets controller system data.
--	Standard	Any object, task, tag, program, or component in your project that is not a safety-related item (that is, standard controller refers generically to a ControlLogix or CompactLogix controller).

Additional Resources

The table below provides a listing of publications that contain important information about GuardLogix controller systems.

Resource	Description
GuardLogix Controller Installation Instructions, publication 1756-IN045	Provides information on installing the GuardLogix controller
GuardLogix Controllers User Manual, publication 1756-UM020	Configuring and programming the GuardLogix system
CompactLogix Controllers Installation Instructions, publication 1768-IN004	Provides information on installing Compact GuardLogix controllers
1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002	Details how to configure, program, and operate a 1768 CompactLogix system, and provides technical specifications.
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides information on the GuardLogix Safety Application instruction set
CompactBlock Guard I/O DeviceNet Safety Module Installation Instructions, publication 1791DS-IN002	Provides information on installing CompactBlock Guard I/O DeviceNet Safety modules
Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Provides information on using Guard I/O DeviceNet Safety modules
Guard I/O EtherNet/IP Safety Modules Installation Instructions, publication 1791ES-IN001	Provides information on installing CompactBlock Guard I/O EtherNet/IP Safety modules
Guard I/O EtherNet/IP Safety Modules User Manual, publication 1791ES-UM001	Provides information on using Guard I/O EtherNet/IP Safety modules
Using ControlLogix in SIL2 Applications Safety Reference Manual, publication 1756-RM001	Describes requirements for using ControlLogix controllers, and GuardLogix standard task, in SIL 2 safety control applications.
Logix5000 General Instruction Set Reference Manual, publication 1756-RM003	Provides information on the Logix5000 Instruction Set
Logix Common Procedures Programming Manual, publication 1756-PM001	Provides information on programming Logix5000 controllers, including managing project files, organizing tags, programming and testing routines, and handling faults
Logix5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on using creating and using standard and safety Add-On Instructions in Logix applications.
ControlLogix System User Manual, publication 1756-UM001	Provides information on using ControlLogix in non-safety applications
DeviceNet Modules in Logix5000 Control Systems User Manual, publication DNET-UM004	Provides information on using the 1756-DNB module in a Logix5000 control system
EtherNet/IP Modules in Logix5000 Control Systems User Manual, publication ENET-UM001	Provides information on using the 1756-ENBT module in a Logix5000 control system
ControlNet Modules in Logix5000 Control Systems User Manual, publication CNET-UM001	Provides information on using the 1756-CNB module in Logix5000 control systems
Logix5000 Controllers Execution Time and Memory Use Reference Manual, publication 1756-RM087	Provides information on estimating the execution time and memory use for instructions
Logix Import Export Reference Manual, publication 1756-RM084	Provides information on using RSLogix 5000 Import/Export utility

You can view or download publications at http://literature.rockwellautomation.com. To order paper copies of technical documentation, contact your local Rockwell Automation distributor or sales representative.

Notes:

Safety Integrity Level (SIL) Concept

Introduction

This chapter introduces you to the Safety Integrity Level (SIL) concept and how the GuardLogix controller meets the requirements for SIL 3 certification.

Topic	Page
SIL 3 Certification	13
Functional Verification Tests	14
GuardLogix Architecture for SIL 3 Applications	15
GuardLogix System Components	16
GuardLogix Certifications	18
GuardLogix PFD and PFH Specifications	19
Safety Integrity Level (SIL) Compliance Distribution and Weight	20
System Reaction Time	21
Safety Task Period and Safety Task Watchdog	21
Contact Information If Device Failure Occurs	22

SIL 3 Certification

1756 and 1768 GuardLogix controller systems are **type-approved** and certified for use in safety applications up to and including SIL 3 according to IEC 61508 and IEC 62061, safety applications up to and including Performance Level PLe (Category 4) according to ISO 13849-1. SIL requirements are based on the standards current at the time of certification.

IMPORTANT When the GuardLogix controller is in the Run or Programming mode and the application has not been validated by the user, the user is responsible for maintaining safe conditions.

In addition, the standard tasks within 1756 GuardLogix controllers can be used either for standard applications or SIL 2 safety applications as described in the Using ControlLogix in SIL 2 Applications Reference Manual, publication 1756-RM001. In either case, do not use SIL 2 or standard tasks and variables to build up safety loops of a higher level. The safety task is the only task certified for SIL 3 applications.

The standard task in 1768 Compact GuardLogix controllers may not be used for SIL 2 safety applications.

RSLogix 5000 programming software is required to create programs for 1756 and 1768 GuardLogix controllers.

The TÜV Rheinland has approved GuardLogix controller systems for use in safety-related applications up to SIL 3, in which the de-energized state is considered to be the safe state. All of the examples related to I/O included in this manual are based on achieving de-energization as the safe state for typical Machine Safety and Emergency Shutdown (ESD) Systems.

IMPORTANT

The system user is responsible for:

- the set-up, SIL rating, and validation of any sensors or actuators connected to the GuardLogix system.
- project management and functional testing.
- access control to the safety system, including password handling.
- programming the application software and the device configurations in accordance with the information in this safety reference manual and the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual publication 1768-UM002.

When applying Functional Safety, restrict access to qualified, authorized personnel who are trained and experienced. The safety-lock function, with passwords, is provided in RSLogix 5000 software.

For information on using the safety-lock feature, refer to the GuardLogix Controllers User Manual, publication 1756-UM020 or the 1768 Compact GuardLogix Controllers User Manual publication 1768-UM002.

Functional Verification Tests

IEC 61508 requires the user to perform various functional verification tests of the equipment used in the system. Functional verification tests are performed at user-defined times. For example, functional verification test intervals can be once a year, once every 15 years, or whatever timeframe is appropriate.

GuardLogix controllers have a functional verification test interval of up to 20 years. Other components of the system, such as Safety I/O modules, sensors, and actuators may have shorter functional verification test intervals. The controller should be included in the functional verification testing of the other components in the safety system.

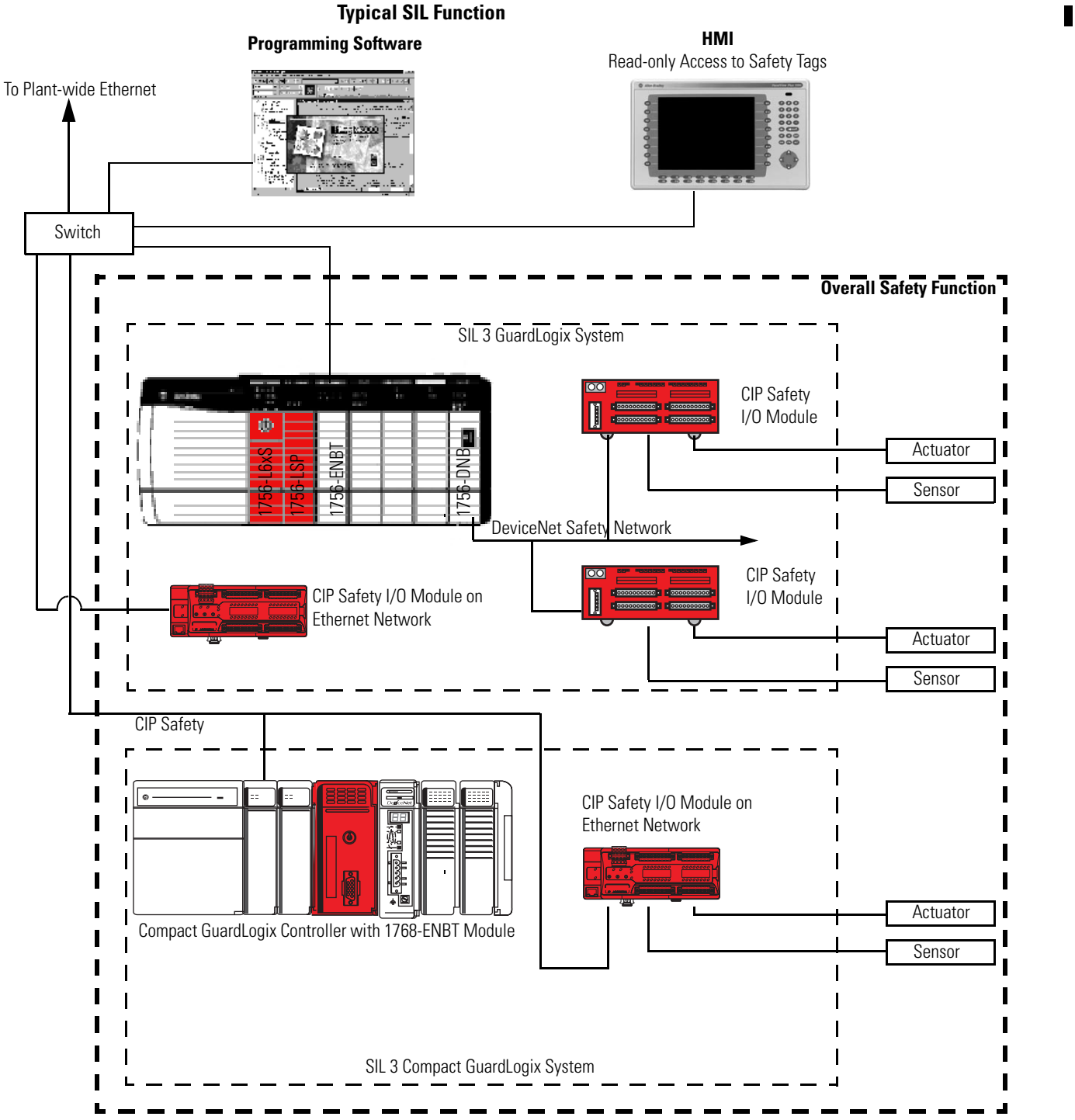
IMPORTANT Your specific applications determine the timeframe for the functional verification test interval. However this is mainly related to Safety I/O modules and field instrumentation.

For more information on the requirements of a functional verification test, see Project Verification Test on pages 57 and 58.

GuardLogix Architecture for SIL 3 Applications

The following illustration shows a typical SIL function, including:

- the overall safety function.
- the GuardLogix portion of the overall safety function.
- how other devices (for example, HMI) are connected, while operating outside the function.



GuardLogix System Components

The tables in this section list SIL 3-certified GuardLogix components for both 1756 and 1768 systems as well as non-SIL 3-certified components that may be used with SIL 3 GuardLogix systems.

For the most current list of GuardLogix controller and CIP Safety I/O modules certified series and firmware revisions, see http://www.rockwellautomation.com/products/certification/safety/. Firmware revisions are available at http://support.rockwellautomation.com/ControlFlash/.

SIL 3-Certified GuardLogix Components

Device Type	Cat. No.	Description	Related Documentation[1]	
			Installation Instructions	User Manual
1756 Primary controller (ControlLogix556*x*S)	1756-L61S	Controller with 2 MB standard, 1 MB safety memory	1756-IN045	1756-UM020
	1756-L62S	Controller with 4 MB standard, 1 MB safety memory		
	1756-L63S	Controller with 8 MB standard, 3.75 MB safety memory		
1756 Safety partner (ControlLogix55SP)	1756-LSP	Safety partner		
1768 Compact GuardLogix Controller (CompactLogix4*x*S)	1768-L43S	Controller with support for two 1768 modules	1768-IN004	1768-UM002
	1768-L45S	Controller with support for four 1768 modules		
CIP Safety I/O modules on DeviceNet networks	For the most current list of certified series and firmware revisions, see the safety certificate at http://www.rockwellautomation.com/products/certification/safety/		1791DS-IN001 1791DS-IN002 1732DS-IN001	1791DS-UM001
CIP Safety I/O modules on EtherNet/IP networks			1791ES-IN001	1791ES-UM001

(1) These publications are available from Rockwell Automation by visiting http://literature.rockwellautomation.com.

Components Suitable for Use With 1768 Compact GuardLogix Controller Safety Systems

Device Type	Cat. No.	Description	Series[1]	Version[1]	Related Documentation[2]	
					Installation Instructions	User Manual
Power supply	1768-PA3	Power supply, ac	N/A	N/A	1768-IN001	None available.
	1768-PB3	Power supply, dc	N/A	N/A		
Communication modules	1768-ENBT	EtherNet/IP bridge module	A	3.1.1	1768-IN002	ENET-UM001
	1734-AENT	POINT I/O Ethernet Adapter	A	3.001	1734-IN590	1734-UM011
	1734-AENTR	POINT I/O Ethernet Adapter	A	3.001	1734-IN040	None available.
	1768-CNB	ControlNet bridge module	A	2.1.1	1768-IN006	CNET-UM001
Programming software	9324-*xxxx*	RSLogix 5000 software	N/A	18	N/A	Consult online help.
CompactFlash Cards	1784-CF64	64MB CompactFlash Card	N/A	N/A	N/A	N/A
	1784-CF128	128MB CompactFlash Card	N/A	N/A	N/A	N/A

(1) This version or later.
(2) These publications are available from Rockwell Automation by visiting http://literature.rockwellautomation.com.

Components Suitable for Use With 1756 GuardLogix Controller Safety Systems

Device Type	Cat. No.	Description	Series[2]	Version[2]	Related Documentation[4]	
					Installation Instructions	User Manual
Chassis	1756-A4, A7, A10, A13, A17	Chassis	B	N/A	1756-IN080	None available.
Power supply	1756-PA72	Power supply, ac	C	N/A	1756-IN596	
	1756-PB72	Power supply, dc	C	N/A		
	1756-PA75	Power supply, ac	B	N/A		
	1756-PB75	Power supply, dc	B	N/A		
	1756-PA75R[1]	Redundant power supply, ac	A	N/A	1756-IN573	
	1756-PB75R	Redundant power supply, dc	A	N/A		
Communication modules	1756-ENBT 1756-EN2T 1756-EN2F	EtherNet/IP bridge module	A A A	3.6 2.005 2.005	1756-IN019 1756-IN603 1756-IN606	ENET-UM001
	1734-AENT	POINT I/O Ethernet Adapter	A	3.001	1734-IN590	1734-UM011
	1756-DNB	DeviceNet bridge module	A	6.2	1756-IN566	DNET-UM004
	1756-CN2	ControlNet bridge module	A	12.1	1756-IN602	CNET-UM001
	1756-CN2R	ControlNet bridge module, redundant media	A	12.1	1756-IN602	CNET-UM001
Programming software	9324-*xxxx*	RSLogix 5000 software	N/A	14[3]	NA	Consult online help.
CompactFlash Cards	1784-CF64	64MB CompactFlash Card	N/A	N/A	N/A	N/A
	1784-CF128	128MB CompactFlash Card	N/A	N/A	N/A	N/A

(1) A 1756-PSCA or 1756-PSCAR redundant power supply chassis adapter is required for use with redundant power supplies.
(2) This version or later.
(3) RSLogix 5000 software, version 15, does not support GuardLogix safety controllers.
(4) These publications are available from Rockwell Automation by visiting http://literature.rockwellautomation.com.

Slots of a SIL 3 system chassis not used by the 1756 SIL 3 system may be populated with other ControlLogix (1756) modules that are certified to the Low Voltage and EMC Directives.

Expansion slots of a SIL 3 system bus that are not used by the 1768 SIL 3 system may be populated with other CompactLogix (1768) modules that are certified to the Low Voltage and EMC Directives.

To find the certificates for the 'Programmable Control – ControlLogix Product Family' and 'Programmable Control – CompactLogix Product Family', refer to http://www.rockwellautomation.com/products/certification/ce/ .

GuardLogix Certifications

This table lists the main GuardLogix certifications. For the full listing of current safety certifications and associated products, refer to http://www.rockwellautomation.com/products/certification/safety/index.html.

Catalog Number	UL 508	UL 1998	ANSI RIA 15.06	NFPA 79	ISO 13849-1:2006 (PLe)	IEC 61508 (SIL 3)	IEC 61511	IEC62061
1756-L61S,1756-L62S, 1756-L63S	X	X	X	X	X	X	X	X
1768-L43S, 1768-L45S	X	X	X	X	X	X	X	X

GuardLogix user documentation typically lists the agency certifications for which the products are approved. If a product has achieved agency certification, it is marked as such on the product labeling. Product certifications are listed in the product's specifications table, similar to the example shown below.

Certification	Description
Functional Safety(1)	Certified by TÜV: capable of SIL 1 to 3, according to IEC 61508, and PLe/Cat. 4 according to ISO 13849-1
	Certified by UL: capable of SIL 3, see UL File E256621.
c-UL-us	UL Listed Industrial Control Equipment, certified for US and Canada. See UL File E65584. UL Listed for Class I, Division 2 Group A,B,C,D Hazardous Locations, certified for U.S. and Canada. See UL File E194810.
CSA	CSA Certified Process Control Equipment. See CSA File LR54689C. CSA Certified Process Control Equipment for Class I, Division 2 Group A,B,C,D Hazardous Locations
FM	FM Approved Equipment for use in Class I Division 2 Group A,B,C,D Hazardous Locations
CE	European Union 2004/108/EC EMC Directive, compliant with: • EN 61000-6-4; Industrial Emissions • EN 61326-1; Meas./Control/Lab., Industrial Requirements • EN 61000-6-2; Industrial Immunity • EN61131-2; Programmable Controllers (Clause 8, Zone A & B)
C-Tick	Australian Radiocommunications Act, compliant with: AS/NZS CISPR 11; Industrial Emissions

(1) When used with specified software versions and as described in the GuardLogix Controller Systems Safety Reference Manual, publication 1756-RM093.

See the Product Certification link at http://www.rockwellautomation.com/products/certification/ for Declarations of Conformity, Certificates, and other certification details.

GuardLogix PFD and PFH Specifications

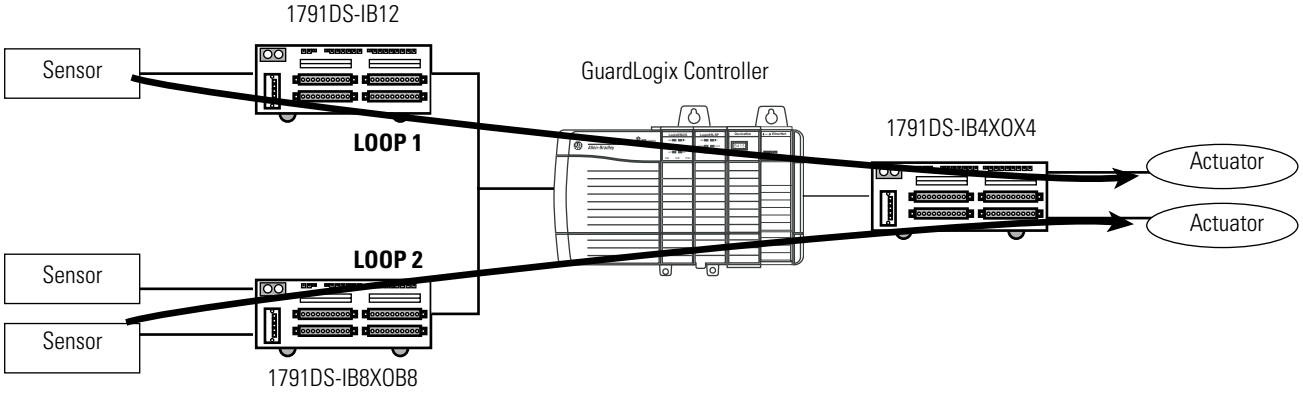
Safety-related systems can be classified as operating in either a low demand mode, or in a high demand/continuous mode. IEC 61508 quantifies this classification by stating that the frequency of demands for operation of the safety system is no greater than once per year in the low demand mode, or greater than once per year in high demand/continuous mode.

The Safety Integrity Level (SIL) value for a low demand safety-related system is directly related to order-of-magnitude ranges of its average probability of failure to satisfactorily perform its safety function on demand or, simply, probability of failure on demand (PFD). The SIL value for a high demand/continuous mode safety-related system is directly related to the probability of a dangerous failure occurring per hour (PFH).

PFD and PFH values are associated with each of the three primary elements making up a safety-related system (the sensors, the logic element, and the actuators). Within the logic element you also have input, processor, and output elements.

For PFD and PFH values and functional verification (proof) test intervals for CIP Safety I/O modules, see Appendix E, Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH) Data.

PFH Example



To determine the logic element PFH for each safety loop in the simple example system shown in the PFH Example, sum the PFH values for each component in the loop. The PFH Equations by Safety Loop table provides a simplified example of PFH value calculations for each safety loop shown in the PFH Example illustration.

PFH Equations by Safety Loop

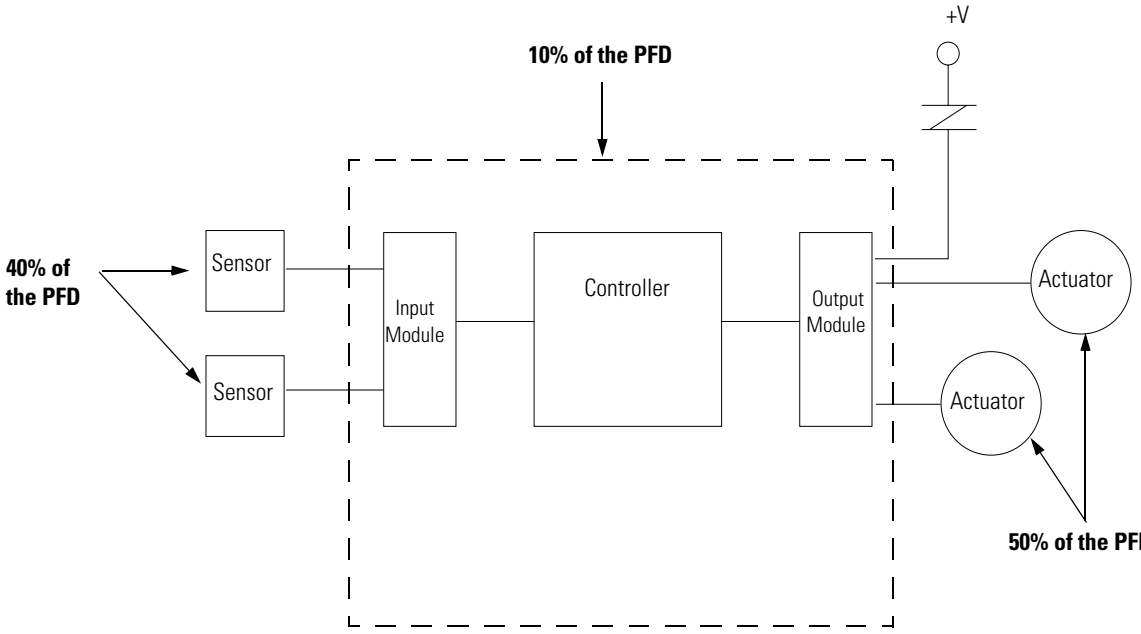
For this loop	Sum the PFH values of these components
Total PFH for loop 1 =	1791DS-IB12 + GuardLogix controller + 1791DS-IB4XOX4
Total PFH for loop 2 =	1791DS-IB8XOB8 + GuardLogix controller + 1791DS-IB4XOX4

When calculating PFH values, you must take into account the specific requirements of your application, including test intervals.

Safety Integrity Level (SIL) Compliance Distribution and Weight

The GuardLogix controller and I/O system may conservatively be assumed to contribute 10% of the reliability burden. A SIL 3 system may need to incorporate multiple inputs for critical sensors and input devices, as well as dual outputs connected in series to dual actuators dependent on SIL assessments for the safety related system.

Reliability Burden



System Reaction Time

The system reaction time is the amount of time from a safety-related event as an input to the system until the system sets corresponding outputs to their safe state. Faults within the system can also have an effect upon the reaction time of the system. The system reaction time is the sum of the following reaction times.

Each of the times listed above is variably dependent on factors such as the type of I/O module and instructions used in the program.

Safety Task Reaction Time

The Safety Task Reaction Time is the worst-case delay from any input change presented to the controller until the processed output is set by the output producer. It is less than or equal to the sum of the safety task period and the safety task watchdog.

Safety Task Period and Safety Task Watchdog

The safety task period is the interval at which the safety task executes.

The safety task watchdog time is the maximum permissible time for safety task processing. If safety task processing time exceeds the safety task watchdog time, a non-recoverable safety fault occurs in the controller and outputs transition to the safe state (off) automatically.

You define the safety task watchdog time, which must be less than or equal to the safety task period.

The safety task watchdog time is set in the task properties window of RSLogix 5000 software. This value can be modified online, regardless of controller mode, but it cannot be changed when the controller is safety-locked or once a safety task signature is created.

Contact Information If Device Failure Occurs

If you experience a failure with any SIL 3-certified device, contact your local Rockwell Automation distributor. With this contact, you can:

- return the device to Rockwell Automation so the failure is appropriately logged for the catalog number affected and a record is made of the failure.
- request a failure analysis (if necessary) to try to determine the cause of the failure.

GuardLogix Controller System

Introduction

Topic	Page
1756 GuardLogix Controller Hardware	23
1768 Compact GuardLogix Controller Hardware	25
CIP Safety Protocol	25
Safety I/O	25
Communication Bridges	26
Programming Overview	28

For a brief listing of components suitable for use in Safety Integrity Level (SIL) 3 applications, see the table on page 16. For more detailed and up-to-date information see http://www.rockwellautomation.com/products/certification/safety/.

When installing a GuardLogix controller, follow the information in the GuardLogix Controllers Installation Instructions, publication 1756-IN045, or CompactLogix Controllers Installation Instructions, publication 1768-IN004.

1756 GuardLogix Controller Hardware

The 1756 GuardLogix controller consists of a primary controller, catalog number 1756-L61S, 1756-L62S, or 1756-L63S, and a safety partner, catalog number 1756-LSP. These two modules work in a 1oo2 architecture to create the SIL 3-capable controller. They are described in the following sections.

Both the primary controller and safety partner perform power-up and run-time functional diagnostic tests of all safety-related components in the controller.

Both also feature status indicators. For details on status indicator operation, refer to the GuardLogix Controllers User Manual, publication 1756-UM020.

IMPORTANT Status indicators are not reliable indicators for safety functions. They should be used only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators to determine operational status.

Primary Controller

The primary controller is the processor that performs standard and safety control functions and communicates with the safety partner for safety-related functions in the GuardLogix control system. The primary controller consists of a central processor, I/O interface, and memory.

Safety Partner

To satisfy SIL 3 requirements, a safety partner, catalog number 1756-LSP, must be installed in the slot immediately to the right of the primary controller. The safety partner is a co-processor that provides redundancy for safety-related functions in the system.

The safety partner is configured by the primary controller. Only a single download of the user program to the primary controller is required. The safety partner's operating mode is controlled by the primary controller.

Chassis

The 1756-A*xx* chassis provides the physical connections between modules and the 1756 GuardLogix system. Any failure, though unlikely, would be detected as a failure by one or more of the active components of the system. Therefore, the chassis is not relevant to the safety discussion.

Power Supplies

These ControlLogix power supplies are suitable for use in SIL 3 applications:

- 1756-PA72 ac power supply
- 1756-PA75 ac power supply
- 1756-PB72 dc power supply
- 1756-PB75 dc power supply
- 1756-PA75R ac power supply (redundant)
- 1756-PB75R dc power supply (redundant)
- 1756-PSCA or 1756-PSCA2 redundant power-supply chassis adapter (required for use with redundant power supplies)

No extra configuration or wiring is required for SIL 3 operation of the ControlLogix power supplies. Any failure would be detected as a failure by one or more of the active components of the GuardLogix system. Therefore, the power supply is not relevant to the safety discussion.

1768 Compact GuardLogix Controller Hardware

The 1768 Compact GuardLogix controllers combine the primary and safety partner controllers in a single controller hardware package to form a SIL-3 capable controller. Compact GuardLogix controllers feature a 1768 backplane and a 1769 backplane to support standard 1769 I/O modules.

Controller	Maximum 1768 Modules (local)	Maximum 1769 I/O Modules (local and remote)
1768-L43S	2	16
1768-L45S	4	30

The 1768 Compact GuardLogix controller is powered by a 1768-PA3 or 1768-PB3 power supply. A 1769-ECR end cap is also required.

CIP Safety Protocol

Safety-related communication between GuardLogix controllers takes place via produced and consumed safety tags. These safety tags use the CIP Safety protocol, which is designed to preserve data integrity during communication.

For more information on safety tags, see Chapter 5, Characteristics of Safety Tags, the Safety Task, and Safety Programs.

Safety I/O

For information on CIP Safety I/O modules for use with GuardLogix controllers, see Chapter 3.

Communication Bridges

These communication interface modules are available to facilitate communication over Ethernet/IP, DeviceNet, and ControlNet networks via the CIP Safety protocol.

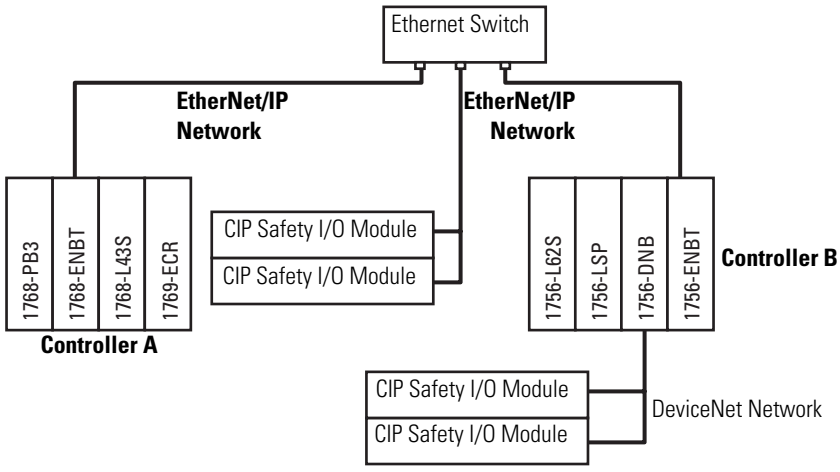
GuardLogix System	Communication Modules
1756	• 1756-ENBT, 1756-EN2T, or 1756-EN2F EtherNet/IP bridge module • 1734-AENT POINT I/O Ethernet Adapter • 1756-DNB DeviceNet bridge module • 1756-CN2 ControlNet bridge module • 1756-CN2R Redundant ControlNet bridge module
1768	• 1768-ENBT • 1734-AENT POINT I/O Ethernet Adapter • 1768-CNB • 1768-CNBR

IMPORTANT Due to the design of the CIP Safety control system, CIP safety bridge devices, like those listed in the table, are not required to be SIL 3-certified.

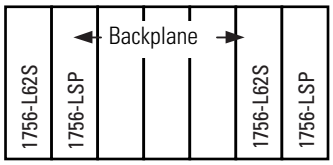
EtherNet/IP Network

Peer-to-peer safety communication between GuardLogix controllers is possible via the EtherNet/IP network through the use of 1756-ENBT, 1756-EN2T, or 1768-ENBT bridge modules. An EtherNet/IP bridge module lets the GuardLogix controller control and exchange safety data with CIP Safety I/O modules on an EtherNet/IP network.

Peer-to-peer Communication via 1756-ENBT Modules and the EtherNet/IP Network



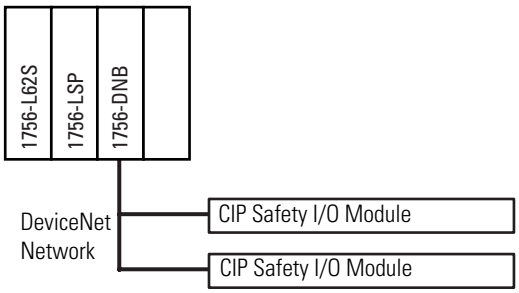
TIP Peer-to-peer safety communication between two 1756 GuardLogix controllers in the same chassis is also possible via the backplane.



DeviceNet Safety Network

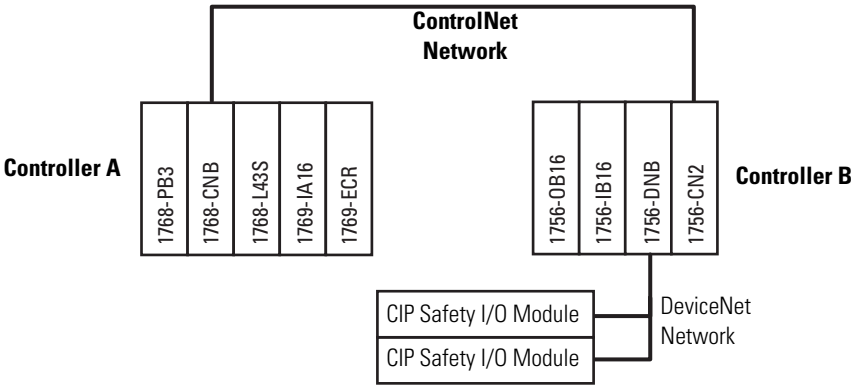
The 1756-DNB DeviceNet bridge module lets the 1756 GuardLogix controller control and exchange safety data with CIP Safety I/O modules on a DeviceNet network.

DeviceNet Communication via a 1756-DNB Module



ControlNet Network

The 1756-CN2 or 1768-CNB module lets the GuardLogix controller produce and consume safety tags over ControlNet networks to other GuardLogix processors or remote CIP Safety I/O networks.



Programming Overview

The programming software for the GuardLogix controller is RSLogix 5000 software.

RSLogix 5000 software is used to define the location, ownership, and configuration of I/O modules and controllers. The software is also used to create, test, and debug application logic. Initially, only relay ladder logic is supported in the GuardLogix safety task.

See Appendix A for information on the set of logic instructions available for safety applications.

Authorized personnel may change an application program, but only by using one of the processes described in Editing Your Safety Application on page 63.

CIP Safety I/O for the GuardLogix Control System

Introduction

Topic	Page
Overview	29
Typical Safety Functions of CIP Safety I/O Modules	29
Reaction Time	31
Safety Considerations for CIP Safety I/O Modules	31

Overview

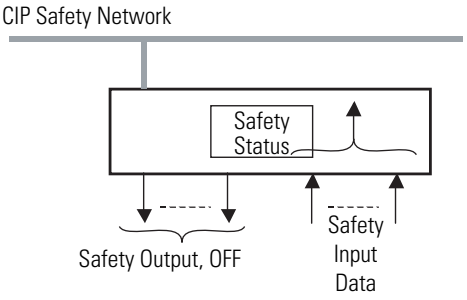
Before operating a GuardLogix safety system containing CIP Safety I/O modules, you must read, understand, and follow the installation, operation, and safety information provided in the publications listed in the SIL 3-Certified GuardLogix Components tables on page 16.

CIP Safety I/O modules can be connected to safety input and output devices, allowing these devices to be monitored and controlled by the GuardLogix controller. For safety data, I/O communication is performed through safety connections using the CIP Safety protocol; safety logic is processed in the GuardLogix controller.

Typical Safety Functions of CIP Safety I/O Modules

The following is treated as the safe state by CIP Safety I/O modules:

- Safety outputs: OFF
- Safety input data to controller: OFF



The CIP Safety I/O modules should be used for applications that are in the safe state when the safety output turns OFF.

Diagnostics

CIP Safety I/O modules perform self-diagnostics when the power is turned ON and periodically during operation. If a diagnostic failure is detected, safety input data (to the controller) and local safety outputs are set to their safe state (OFF).

Status Data

In addition to safety input and output data, CIP Safety I/O modules support status data to monitor module and I/O circuit health. Refer to your module's product documentation for specific product capabilities.

Status Indicators

The CIP Safety I/O modules include status indicators. For details on status indicator operation, refer to the product documentation for your specific module.

On- or Off-delay Function

Some CIP Safety I/O modules may support On-delay and Off-delay functions for input signals. Depending upon your application, you may need to include Off-delay, On-delay, or both when calculating system reaction time.

See Appendix C for information on system reaction time.

Reaction Time

The input reaction time is the time from when the signal changes on an input terminal to when safety data is sent to the GuardLogix controller.

The output reaction time is the time from when safety data is received from the GuardLogix controller to when the output terminal changes state.

For information on determining the input and output reaction times, refer to the product documentation for your specific CIP Safety I/O module.

See Appendix C for information on calculating the system reaction time.

Safety Considerations for CIP Safety I/O Modules

You must commission all devices with a node or IP address and communication rate, if necessary, before their installation on a safety network.

Ownership

Each CIP Safety I/O module in a GuardLogix system is owned by one GuardLogix controller. Multiple GuardLogix controllers and multiple CIP Safety I/O modules can be used without restrictions in chassis or on networks as needed. When a controller owns an I/O module, it stores the module's configuration data, as defined by the user. This controls how the modules operate in the system.

From a control standpoint, safety output modules can only be controlled by one controller. Each safety input module is also owned by a single controller; however safety input data can be shared (consumed) by multiple GuardLogix controllers.

Safety I/O Configuration Signature

The configuration signature defines the module's configuration. It can be read and monitored. The configuration signature is used to uniquely identify a module's configuration. When using a GuardLogix controller, you do not have to monitor this signature. It is monitored automatically by the GuardLogix controller.

I/O Module Replacement

The replacement of safety devices requires that the replacement device be configured properly and that the replacement device's operation be user-verified.

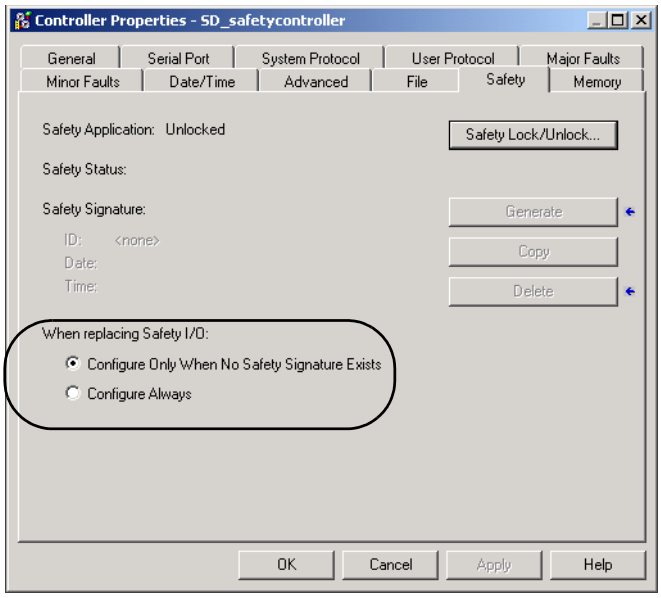
ATTENTION

During replacement or functional testing of a module, the safety of the system must not rely on any portion of the affected module.

Two options for I/O module replacement are available on the Safety tab of the Controller Properties dialog in RSLogix 5000 software:

- Configure Only When No Safety Signature Exists
- Configure Always

Safety I/O Replacement Options



Configure Only When No Safety Signature Exists

This setting instructs the GuardLogix controller to configure a safety module only when the safety task does not have a safety task signature, and the replacement module is in an out-of-box condition, meaning that a safety network number does not exist in the safety module.

If the safety task has a safety task signature, the GuardLogix controller only configures the replacement CIP Safety I/O module if the module already has the correct safety network number, the module electronic keying is correct, and the node or IP Address is correct.

Configure Always

The GuardLogix controller will always attempt to configure a replacement CIP Safety I/O module if the module is in an out-of-box condition, meaning that a safety network number does not exist in the replacement safety module, and the node number and I/O module keying matches the controller's configuration.

ATTENTION

Enable the Configure Always feature only if the entire routable CIP Safety control system is not being relied on to maintain SIL 3 behavior during the replacement and functional testing of a module.

If other parts of the CIP Safety control system are being relied upon to maintain SIL 3, make sure that the controller's Configure Always feature is disabled.

It is your responsibility to implement a process to make sure proper safety functionality is maintained during device replacement.

ATTENTION

Do not place any modules in the out-of-box condition on any CIP Safety network when the Configure Always feature is enabled, except while following the module replacement procedure in the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002.

Notes:

CIP Safety and the Safety Network Number

Introduction

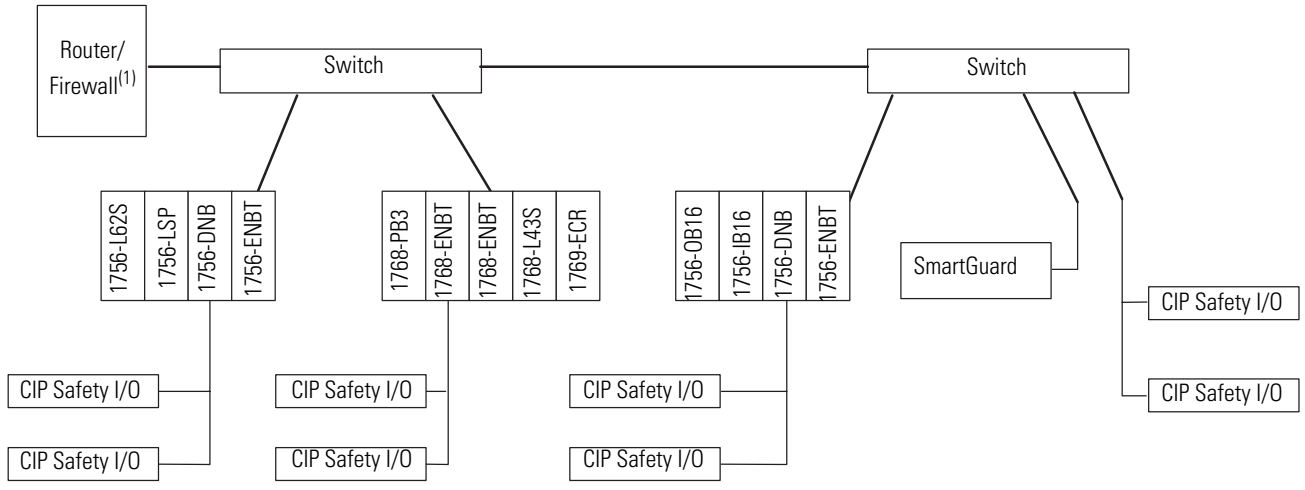
To understand the safety requirements of a CIP Safety control system, including the safety network number (SNN), you must first understand how communication is routable in CIP control systems.

Topic	Page
The Routable CIP Safety Control System	35
Considerations for Assigning the Safety Network Number (SNN)	38

The Routable CIP Safety Control System

The CIP Safety control system represents a set of interconnected CIP Safety devices. The routable system represents the extent of potential mis-routing of packets from an originator to a target within the CIP Safety control system. The system is isolated such that there are no other connections into the system. For example, because the system below cannot be interconnected to another CIP Safety system through a larger, plant-wide Ethernet backbone, it illustrates the extent of a routable CIP Safety system.

CIP Safety System Example



(1) The router or firewall is set up to limit traffic.

Unique Node Reference

The CIP Safety protocol is an end-node to end-node safety protocol. The CIP Safety protocol allows the routing of CIP Safety messages to and from CIP Safety devices through non-certified bridges, switches, and routers.

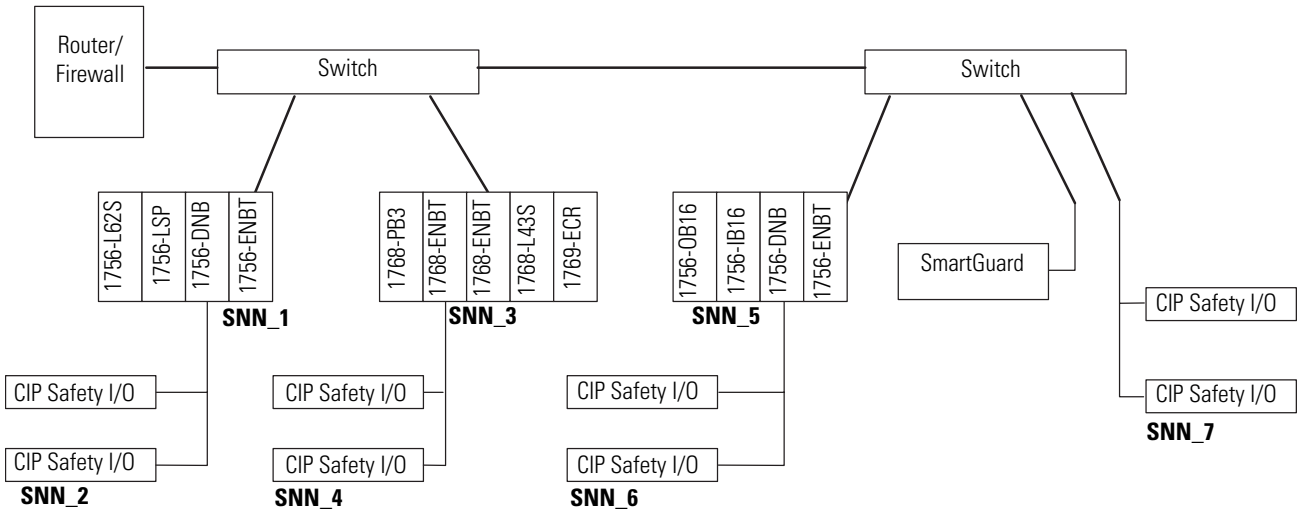
To prevent errors in non-certified bridges, switches, or routers from becoming dangerous, each end node within a routable CIP Safety control system must have a unique node reference. The unique node reference is a combination of a safety network number (SNN) and the node address of the node.

Safety Network Number

The safety network number (SNN) is assigned by software or by the user. Each CIP Safety network that contains Safety I/O nodes must have at least one unique SNN. Each ControlBus chassis that contains one or more safety devices must have at least one unique SNN. Safety network numbers assigned to each safety network or network sub-net must be unique.

TIP More than one SNN can be assigned to a CIP Safety subnet or a ControlBus chassis that contains more than one safety device. However, for simplicity, we recommend that each CIP Safety subnet have one and only one unique SNN. This is also the case for each ControlBus chassis.

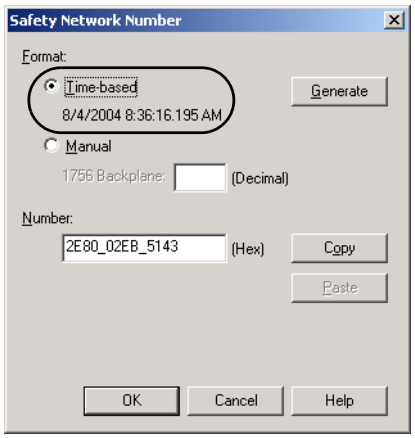
CIP Safety Example with More Than One SNN

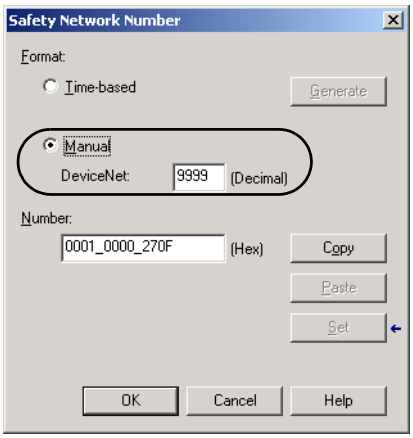


Each CIP Safety device must be configured with an SNN. Any device that originates a safety connection to another safety device must be configured with the SNN of the target device. If the CIP Safety system is in the start-up process prior to the functional safety testing of the system, the originating device may be used to set the unique node reference into the device.

The SNN used by the system is a 6-byte hexadecimal number. The SNN can be set and viewed in one of two formats: time-based or manual. When the time-based format is selected, the SNN represents a localized date and time. When the manual format is selected, the SNN represents a network type and a decimal value from 1…9999.

SNN Formats





The assignment of a time-based SNN is automatic when creating a new GuardLogix safety controller project and adding new Safety I/O modules.

Manual manipulation of an SNN is required in the following situations:

- If safety consumed tags are used.
- If the project will consume safety input data from a module whose configuration is owned by some other safety device.
- If a safety project is copied to a different hardware installation within the same routable CIP Safety system.

IMPORTANT If you assign an SNN manually, take care to ensure that system expansion does not result in duplication of SNN and node address combinations.

Considerations for Assigning the Safety Network Number (SNN)

The assignment of the SNN is dependent upon factors including the configuration of the controller or CIP Safety I/O module.

Safety Network Number (SNN) for Safety Consumed Tags

When a safety controller that contains produced safety tags is added to the I/O Configuration tree, the SNN of the producing controller must be entered. The SNN may be copied from the producing controller's project and pasted into the new controller being added to the I/O Configuration tree.

Refer to the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002, for information on how to copy and paste an SNN.

Safety Network Number (SNN) for Out-of-box Modules

Out-of-box CIP Safety I/O modules do not have an SNN. The SNN is set when a configuration is sent to the module by the GuardLogix controller that owns the module.

IMPORTANT To add a CIP Safety I/O module to a configured GuardLogix system (the SNN is present in the GuardLogix controller), the replacement CIP Safety module should have the correct SNN applied before it is added to the CIP Safety network.

Safety Network Number (SNN) for Safety Module with a Different Configuration Owner

When a CIP Safety I/O module is owned by a different GuardLogix controller (controller B), and then is added to another GuardLogix project (controller A project), RSLogix 5000 software assigns the SNN based on the current project. Since the current project (controller A project) is not the true configuration owner, you need to copy the original SNN (controller B project) into the configuration in controller A's project. This is easy to do with standard copy and paste commands. The result is that the CIP Safety I/O module produces data to two GuardLogix controllers at the same time. You can do this for a maximum of 16 controllers.

Refer to the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002, for information on changing, copying, and pasting safety network numbers.

Safety Network Number (SNN) when Copying a Safety Project

ATTENTION

If a safety project is copied for use in another project with different hardware or in a different physical location, and the new project is within the same routable CIP Safety system, every SNN must be changed in the second system. SNN values must not be repeated.

Refer to the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002, for information on changing the SNN.

Notes:

Characteristics of Safety Tags, the Safety Task, and Safety Programs

Introduction

This chapter explains how to use the standard and safety components of the GuardLogix system.

Topic	Page
Differentiate Between Standard and Safety	41
SIL 2 Safety Applications	42
SIL3 Safety – the Safety Task	47
Safety Programs	49
Safety Routines	50
Safety Tags	50
Additional Resources	52

Differentiate Between Standard and Safety

Because it is a Logix series controller, both standard (non-safety-related) and safety-related components can be used in the GuardLogix control system.

You can perform standard automation control from standard tasks within a GuardLogix project. 1756 GuardLogix controllers provide the same functionality as other 1756 ControlLogix series controllers. 1768 Compact GuardLogix controllers provide the same functionality as other 1768-L4*x* CompactLogix controllers. What differentiates 1756 and 1768 GuardLogix controllers from standard controllers is that they provide a SIL 3-capable safety task.

However, a logical and visible distinction is required between the standard and safety-related portions of the application. RSLogix 5000 software provides this differentiation via the safety task, safety programs, safety routines, safety tags, and safety I/O modules. You can implement both SIL 2 and SIL 3 levels of safety control with the safety task of the GuardLogix controller.

SIL 2 Safety Applications

You can perform SIL 2 safety control by using the 1756 or 1768 GuardLogix controller's safety task.

Because 1756 GuardLogix controllers are part of the ControlLogix series of processors, you can perform SIL 2 safety control with a 1756 GuardLogix controller by using standard tasks or the safety task. This capability provides unique and versatile safety control options, since most applications have a higher percentage of SIL 2 safety functions than SIL 3 safety functions.

SIL 2 Safety Control in the Safety Task

The 1756 and 1768 GuardLogix safety task can be used to provide SIL 2 as well as SIL 3 safety functions. If SIL 3 safety functions need to be performed at the same time as SIL 2 safety functions, you must fulfill the requirements defined in the SIL3 Safety – the Safety Task, Safety Programs, and Safety Routines sections of this chapter, as well as the SIL 2 requirements listed in this section.

SIL 2 Safety Logic

From a GuardLogix safety control perspective, the biggest difference between SIL 2 and SIL 3 safety-rated devices is that SIL 2 is generally single-channel, while SIL 3 is typically dual-channel. When using safety-rated I/O, which is required by the safety task, SIL 2 safety can be single-channel, reducing system complexity.

IMPORTANT If a combination of SIL 2 and SIL 3 safety functions are used at the same time within the safety task, you must prevent SIL 2 input signals from directly controlling SIL 3 safety functions. This can be done by using specific safety task programs or routines to separate SIL 2 and SIL 3 safety functions.

Within the safety task, RSLogix 5000 software includes a set of safety-related ladder-logic instructions. In addition to these safety-rated ladder logic instructions, GuardLogix controllers feature application-specific SIL 3-rated safety instructions. All of these logic instructions may be used in Cat 1…4 and SIL 1…3 safety functions.

For SIL 2-only safety, a safety task signature is not required. However, if any SIL 3 safety functions are used within the safety task, a safety task signature is required.

Safety-locking the safety task once testing is completed is recommended for SIL 2 applications. Locking the safety task enables additional security features. You may also use FactoryTalk Security and RSLogix 5000 routine source protection to limit access to safety-related logic.

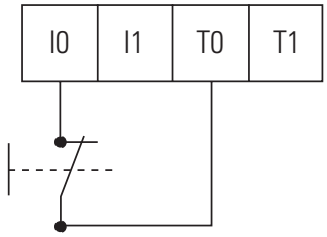
For more information on generating a safety task signature and safety-locking the safety task, refer to the GuardLogix Controllers User Manual, publication 1756-UM020, or the Compact GuardLogix Controllers User Manual, publication 1768-UM002.

SIL 2 Safety Inputs

CompactBlock Guard I/O (1791-series) and ArmorBlock Guard I/O (1732-series) safety input modules support single-channel SIL 2 safety input circuits. Since these modules are also rated for SIL 3 operation, mixing SIL 2 and SIL 3 circuits on the same module is allowed, provided you follow these guidelines.

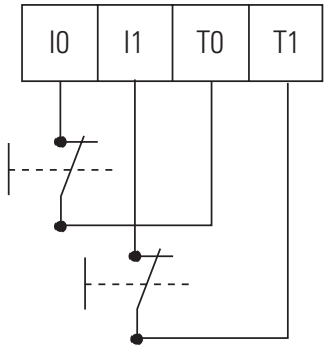
These two wiring examples show how to wire SIL 2 safety circuits to Guard I/O safety input modules. These examples make use of onboard test sources (T0…T*x*) that are resident on all 1791 and 1732 safety input modules.

Input Wiring



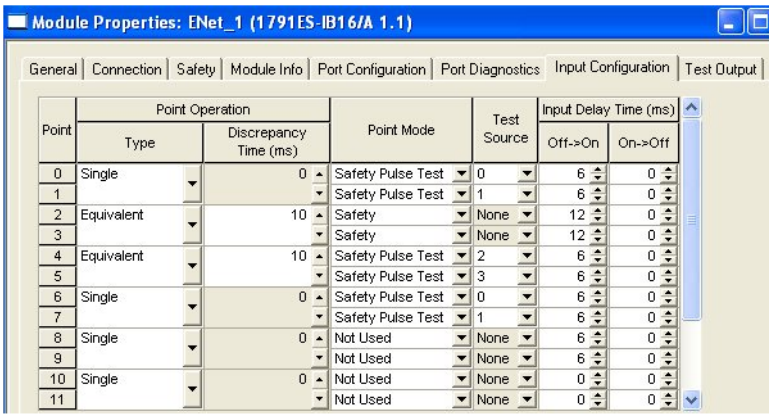
Guard I/O modules group inputs in pairs to facilitate Cat 3, Cat 4, and SIL 3 safety functions. For use in Cat 1, Cat 2, and SIL 2 safety functions, module inputs should still be used in pairs as illustrated. Two SIL 2 safety functions are shown wired to inputs I0 and I1 using test sources T0 and T1, respectively.

Input Wiring in Pairs



For Cat 1, Cat 2, and SIL 2 safety functions, the Guard I/O safety modules need specific configurations within the GuardLogix project. In this example, inputs 0, 1, 6, 7, 8, 9, 10, and 11 are part of a CAT 1, 2 or SIL 2 safety function. Inputs 2 and 3, as well as 4 and 5 are part of a CAT 3, CAT 4, or SIL 3 safety function.

Input Configuration


Module Properties: ENet_1 (1791ES-IB16/A 1.1)
General
Connection
Safety
Module Info
Port Configuration
Port Diagnostics
Input Configuration
Test Output
Point
Point Operation
Type
Discrepancy Time (ms)
Point Mode
Test Source
Input Delay Time (ms)
Off->On
On->Off
0 Single 0 Safety Pulse Test 0 6 0
1 Safety Pulse Test 1 6 0
2 Equivalent 10 Safety None 12 0
3 Safety None 12 0
4 Equivalent 10 Safety Pulse Test 2 6 0
5 Safety Pulse Test 3 6 0
6 Single 0 Safety Pulse Test 0 6 0
7 Safety Pulse Test 1 6 0
8 Single 0 Not Used None 6 0
9 Not Used None 6 0
10 Single 0 Not Used None 0 0
11 Not Used None 0 0

Field	Value
Type	Single
Discrepancy Time	N/A
Point Mode	Safety Pulse Test
Test Source	Set values based on how the field device is physically wired to the module. To make sure the test source is properly enabled, open and view settings on the Test Output tab.
Input Delay Time	User input based on field device characteristics.

IMPORTANT The onboard pulse test outputs (T0…Tx) are typically used with field devices that have mechanical contacts. If a safety device that has electronic outputs is used (feeding safety inputs), they must have the appropriate safety ratings.

IMPORTANT If you are using GuardLogix Safety Application Instructions, be sure to configure your safety input modules as single, not equivalent or complementary. These instructions provide all dual-channel functionality necessary for PLd (Cat. 3) or PLe (Cat. 4) safety functions.

Refer to the GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095.

SIL 2 Safety Control in Standard Tasks (1756 GuardLogix Controllers Only)

Because of the quality and amount of diagnostics built into the 1756 ControlLogix series of controllers, you can perform SIL 2 safety functions from within standard tasks. This is also true for 1756 GuardLogix controllers.

To perform SIL 2 safety control within a GuardLogix standard task, you must abide by requirements defined in the Using ControlLogix in SIL 2 Applications Safety Reference Manual, publication 1756-RM001.

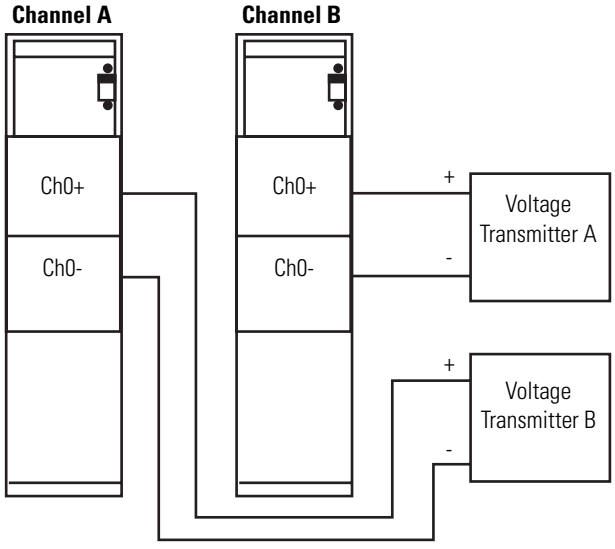
IMPORTANT You may not use the standard task in a 1768 Compact GuardLogix controller for SIL-2 safety applications.

EN50156 Compliance With 1756 ControlLogix SIL 2 Safety Inputs in Dual-channel Configurations with 1756 GuardLogix Controllers

Dual-channel configuration is required for compliance in certain safety-related applications, including burner-related safety functions. These examples provide guidelines for satisfying EN50156 SIL 2 dual-channel requirements.

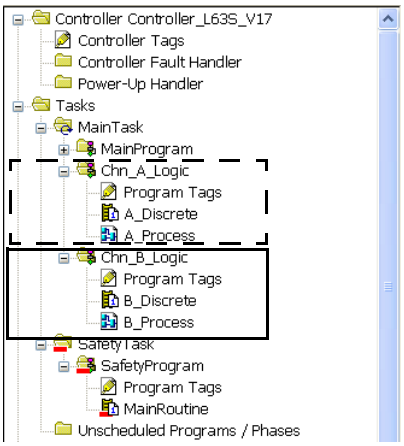
SIL 2 Dual-channel Inputs (Standard Side of 1756 GuardLogix Controllers)

You must implement clear and easily-identifiable separation between both input channels and adhere to all existing SIL 2 requirements as defined in Using ControlLogix in SIL 2 Applications, publication 1756-RM001.



SIL 2 Input Data

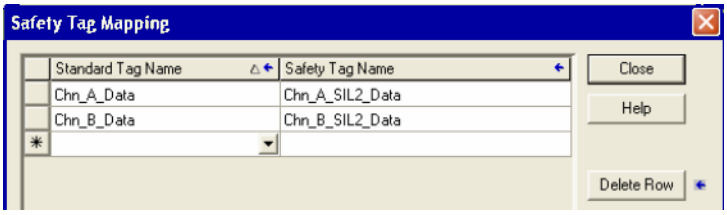
Keep channel A and channel B input data separate at all times. This example illustrates one method for separating channel A and channel B data in your application. Any logic processing that needs to occur must follow ControlLogix SIL 2 guidelines.



IMPORTANT Do not perform safety-specific functions within these routines. Safety evaluation must be handled within the 1756 GuardLogix safety task.

Transferring SIL 2 Data Into the Safety Task

To transfer channel A and channel B SIL 2 safety data into the GuardLogix safety task, use the safety tag mapping functionality in RSLogix 5000 software. The tag names used here are for example purposes. Implement and follow naming conventions that are appropriate for your application.



TIP To use the safety tag mapping feature, choose Map Safety Tags from the Logic menu in RSLogix 5000 software.

Safety Functions Within the 1756 GuardLogix Safety Task

Follow these guidelines for using SIL 2 and SIL 3 safety functions within the safety task:

IMPORTANT You must not use SIL 2 data to directly control a SIL 3 output.

- All available safety application instructions may be used.
- SIL 3 safety input modules (that is , Guard I/O modules) may be used with single-channel configuration for SIL 2 safety functions.
- Use of the safety task signature and safety-locking the application is recommended.

SIL 2 Outputs

Follow these guidelines for SIL 2 outputs:

- Guard I/O output modules used for SIL 2 safety outputs must be configured for dual-channel operation.
- All Guard I/O output modules are approved for use in SIL 2 applications.
  - 1732DS-IB8XOBV4
  - 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  - 1791DS-IB4XOW4
  - 1791DS-IB8XOB8
  - 1734-OB8S

IMPORTANT You cannot use Flex or 1756 output modules in EN 50156 SIL 2 applications.

SIL3 Safety – the Safety Task

Creation of a GuardLogix project automatically creates a single safety task. The safety task has these additional characteristics:

- GuardLogix controllers are the only controllers that support the safety task.
- The safety task cannot be deleted.
- GuardLogix controllers support a single safety task.
- Within the safety task, you can schedule multiple safety programs composed of multiple safety routines.
- You cannot schedule or execute standard routines from within the safety task.

The safety task is a periodic timed task with a user-selectable task priority and watchdog. In most cases, it is the controller's top priority and the user-defined program watchdog must be set to accommodate fluctuations in the execution of the safety task.

Safety Task Limitations

You specify both the safety task period and the safety task watchdog. The safety task period is the period at which the safety task executes. The safety task watchdog is the maximum time allowed from the start of safety task scheduled execution to its completion.

For more information on the safety task watchdog, see Appendix C, Reaction Times.

The safety task period is limited to a maximum of 100 ms and cannot be modified online. Make sure that the safety task has enough time to finish before it is triggered again. Safety task watchdog timeout, a non-recoverable safety fault in the GuardLogix controller, occurs if the safety task is triggered while it is still executing from the previous trigger.

See Chapter 7, Monitor Status and Handle Faults, for more information.

Safety Task Execution Details

The safety task executes in the same manner as standard periodic tasks, with the following exceptions:

- The safety task does not begin executing until the primary controller and safety partner have established their control partnership and the coordinated system time (CST) is synchronized. However, standard tasks begin executing as soon as the controller transitions to Run mode.
- Although the configurable range of the requested packet interval (RPI) for safety inputs and safety consumed tags is 1…100 ms, safety input tags and safety-consumed tags are updated only at the beginning of safety task execution. This means that even though the I/O RPI can be faster than the safety task period, the data does not change during safety task execution. The data is read only once at the beginning of the safety task execution.

- Safety input values are frozen at the start of safety task execution. As a result, timer-related instructions, such as TON and TOF, will not update during a single safety task execution. They will keep accurate time from one task execution to another, but the accumulated time will not change during safety task execution.

ATTENTION

This behavior differs from standard Logix task execution, but is similar to PLC or SLC behavior.

- For standard tags that are mapped to safety tags, the standard tag values are copied into safety memory at the start of the safety task and do not change during safety task execution.
- Safety output tag (output and produced) values are updated at the conclusion of safety task execution
- The safety task responds to mode changes (for example, Run to Program or Program to Run) at timed intervals. As a result, the safety task may take more than one task period, but always less than two, to make a mode transition.

IMPORTANT

While safety-unlocked and without a safety task signature, the controller prevents simultaneous write access to safety memory from the safety task and communication commands. As a result, the safety task can be held off until a communication update completes. The time required for the update varies by tag size. Therefore, safety connection and/or safety watchdog timeouts could occur. (For example, if you make online edits when the safety task rate is set to 1 ms, a safety watchdog timeout could occur.)

To compensate for the hold-off time due to a communication update, add 2 ms to the safety watchdog time.

When the controller is safety-locked or a safety task signature exists, the situation described in this note cannot occur.

Safety Programs

A safety program has all the attributes of a standard program, except that it can be scheduled only in the safety task. A safety program may also define program-scoped safety tags. A safety program may be scheduled or unscheduled.

A safety program can contain only safety components. All of the routines in a safety program are safety routines. A safety program cannot contain standard routines or standard tags.

Safety Routines

Safety routines have all the attributes of standard routines, except that they can exist only in safety programs. One safety routine may be designated as the main routine. Another safety routine may be designated as the fault routine. Only safety-certified instructions may be used in safety routines.

For a listing of safety instructions, see Appendix A.

ATTENTION

To preserve SIL 3, you must make sure that your safety logic does not attempt to read or write standard tags.

Safety Tags

The GuardLogix control system supports the use of both standard and safety tags in the same project. However, the programming software operationally differentiates standard tags from safety tags.

Safety tags have all the attributes of standard tags with the addition of mechanisms to provide SIL 3 data integrity.

Valid Data Types for Safety Tags

- AUX_VALVE_CONTROL
- BOOL
- CAM_PROFILE
- CAMSHAFT_MONITOR
- CB_CONTINUOUS_MODE
- CB_CRANKSHAFT_POS_MONITOR
- CB_INCH_MODE
- CB_SINGLE_STROKE_MODE
- CONFIGURABLE_ROUT
- CONNECTION_STATUS
- CONTROL
- COUNTER
- DCI_MONITOR
- DCI_START
- DCI_STOP
- DCI_STOP_TEST
- DCI_STOP_TEST_LOCK
- DCI_STOP_TEST_MUTE
- DINT
- DIVERSE_INPUT
- EIGHT_POS_MODE_SELECTOR
- EMERGENCY_STOP
- ENABLE_PENDANT
- EXT_ROUTINE_CONTROL
- EXT_ROUTINE_PARAMETERS
- FBD_BIT_FIELD_DISTRIBUTE
- FBD_CONVERT
- FBD_COUNTER
- FBD_LOGICAL
- FBD_MASK_EQUAL
- FBD_MASKED_MOVE
- FBD_TIMER
- FIVE_POS_MODE_SELECTOR
- INT
- LIGHT_CURTAIN
- MAIN_VALVE_CONTROL
- MANUAL_VALVE_CONTROL
- MUTING_FOUR_SENSOR_BIDIR
- MUTING_TWO_SENSOR_ASYM
- MUTING_TWO_SENSOR_SYM
- MOTION_INSTRUCTION
- PHASE
- PHASE_INSTRUCTION
- REDUNDANT_INPUT
- REDUNDANT_OUTPUT
- SAFETY_MAT
- SERIAL_PORT_CONTROL
- SFC_ACTION
- SFC_STEP
- SFC_STOP
- SINT
- STRING
- THRS_ENHANCED
- TIMER
- TWO_HAND_RUN_STATION

IMPORTANT

Aliasing between standard and safety tags is prohibited in safety applications.

Tags classified as safety tags are either controller-scoped or program-scoped. Controller-scoped safety tags can be read by either standard or safety logic or other communication devices, but can only be written to by safety logic or another GuardLogix safety controller. Program-scoped safety tags are only accessible by local safety routines. These are routines that reside within the safety program.

Tags associated with Safety I/O and produced or consumed safety data must be controller-scoped safety tags.

IMPORTANT Any controller-scoped safety tag is readable by any standard routine, but the update rate is based on the execution of the safety task. This means that safety tags are updated at the safety task periodic rate, which is different from standard tag behavior.

Standard Tags in Safety Routines (Tag Mapping)

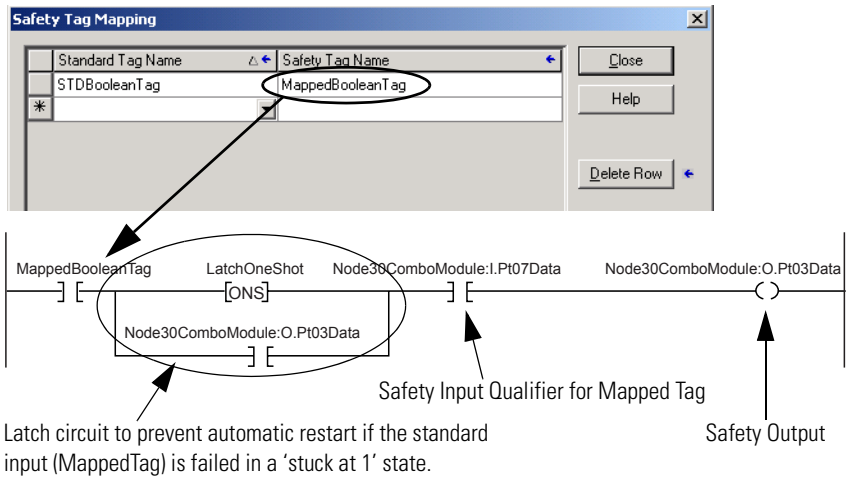
Controller-scoped standard tags can be mapped into safety tags, providing you with a mechanism to synchronize standard and safety actions.

ATTENTION

When using standard data in a safety routine, you are responsible for providing a reliable means of ensuring that the data is used in an appropriate manner. Using standard data in a safety tag does not make it safety data. You must not directly control a safety output with standard tag data.

This example illustrates how to qualify the standard data with safety data.

Qualify Standard Data with Safety Data



Additional Resources

Resource	Description
Logix5000 Controllers Design Considerations Reference Manual, publication 1756-RM094	Provides information on managing tasks and the effects of task execution and timing on user data
GuardLogix Controllers User Manual, publication 1756-UM020	Contains information on how to map tags
1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002	Contains information on how to map tags

Safety Application Development

Introduction

Topic	Page
Safety Concept Assumptions	53
Basics of Application Development and Testing	53
Commissioning Life Cycle	54
Downloading the Safety Application Program	61
Uploading the Safety Application Program	61
Online Editing	61
Storing and Loading a Project from Nonvolatile Memory	62
Force Data	62
Inhibit a Module	63
Editing Your Safety Application	63

Safety Concept Assumptions

The safety concept assumes that:

- if you are responsible for creating, operating, and maintaining the application, you are fully qualified, specially trained, and experienced in safety systems.
- you apply the logic correctly, meaning that programming errors can be detected. Programming errors can be detected by strict adherence to specifications, programming and naming rules.
- you perform a critical analysis of the application and use all possible measures to detect a failure.
- you confirm all application downloads via a manual check of the safety task signature.
- you perform a complete functional test of the entire system before the operational startup of a safety-related system.

Basics of Application Development and Testing

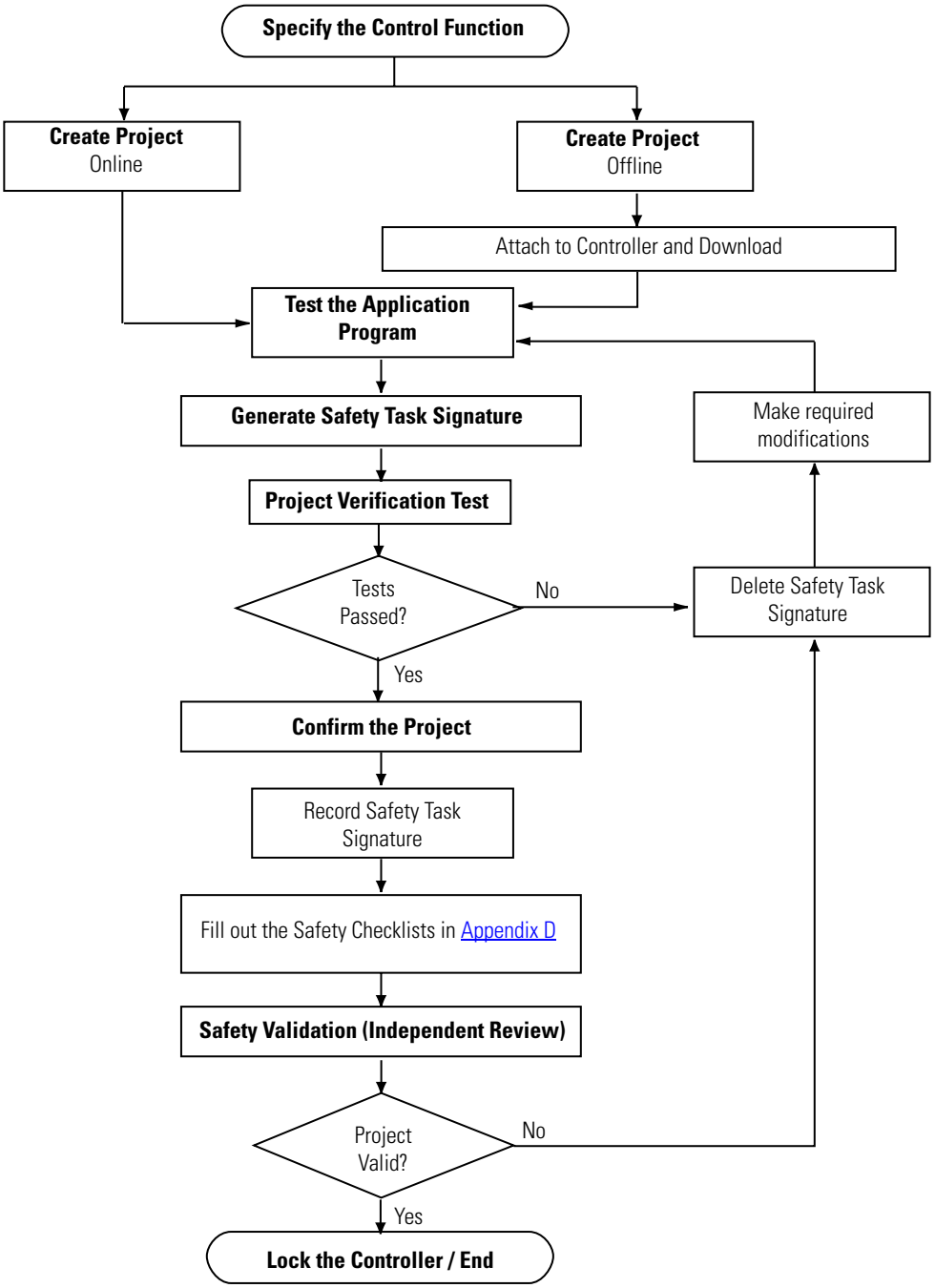
The application program for the intended SIL 3 system should be developed by the system integrator or a user trained and experienced in safety applications. The developer must follow good design practices:

- Use functional specifications, including flow charts, timing diagrams and sequence charts.
- Perform a program review.
- Perform program validation.

Commissioning Life Cycle

The flowchart below shows the steps required for commissioning a GuardLogix system. The items in bold text are explained in the following sections.

Commission the System



Specification of the Control Function

You must create a specification for your control function. Use this specification to verify that program logic correctly and fully addresses your application's functional and safety control requirements. The specification may be presented in a variety of formats, depending on your application. However, the specification must be a detailed description that includes (if applicable):

- sequence of operations.
- flow and timing diagrams.
- sequence charts.
- program description.
- program print out.
- written descriptions of the steps with step conditions and actuators to be controlled. This includes:
  - input definitions.
  - output definitions.
  - I/O wiring diagrams and references.
  - theory of operation.
- matrix or table of stepped conditions and the actuators to be controlled, including the sequence and timing diagrams.
- definition of marginal conditions, for example, operating modes and EMERGENCY STOP.

The I/O portion of the specification must contain the analysis of field circuits, that is, the type of sensors and actuators.

- Sensors (Digital or Analog)
  - Signal in standard operation (dormant current principle for digital sensors, sensors OFF means no signal)
  - Determination of redundancies required for SIL levels
  - Discrepancy monitoring and visualization, including your diagnostic logic
- Actuators
  - Position and activation in standard operation (normally OFF)
  - Safe reaction/positioning when switching OFF or power failure
  - Discrepancy monitoring and visualization, including your diagnostic logic

Create the Project

The logic and instructions used in programming the application must be:

- easy to understand.
- easy to trace.
- easy to change.
- easy to test.

All logic should be reviewed and tested. Keep safety-related logic and standard logic separate.

Label the Program

The application program is clearly identified by one of the following:

- Name
- Date
- Revision
- Any other user identification

Test the Application Program

This step consists of any combination of Run and Program mode, online or offline edits, upload and download, and informal testing that is required to get an application running properly.

Generate the Safety Task Signature

The safety task signature uniquely identifies each project, including its logic, data, and tags. The safety task signature is composed of an ID (identification number), date, and time.

You can generate the safety task signature if all of the following conditions are true:

- RSLogix 5000 software is online with the controller.
- The controller is in program mode.
- The controller is safety-unlocked.
- The controller has no safety forces or pending online safety edits.
- The safety task status is OK.

Once application program testing is complete, you must generate the safety task signature. The programming software automatically uploads the safety task signature after it is generated.

IMPORTANT To verify the integrity of every download, you must manually record the safety task signature after initial creation and check the safety task signature after every download to make sure that it matches the original.

You can delete the safety task signature only when the GuardLogix controller is safety-unlocked and, if online, the keyswitch is in the REM or PROG position.

When a safety task signature exists, the following actions are not permitted within the safety task:

- Online or offline programming or editing of safety components
- Forcing Safety I/O
- Data manipulation (except through routine logic or another GuardLogix controller)

Project Verification Test

To check the application program for adherence to the specification, you must generate a suitable set of test cases covering the application. The set of test cases must be filed and retained as the test specification.

You must include a set of tests to prove the validity of the calculations (formulas) used in your application logic. Equivalent range tests are acceptable. These are tests within the defined value ranges, at the limits, or in invalid value ranges. The necessary number of test cases depends on the formulas used and must comprise critical value pairs.

Active simulation with sources (field devices) must also be included, since it is the only way to verify that the sensors and actuators in the system are wired correctly. Verify the operation of programmed functions by manually manipulating sensors and actuators.

You must also include tests to verify the reaction to wiring faults and network communication faults.

Project verification includes required functional verification tests of fault routines, input and output channels, to ensure that the safety system operates properly.

To perform a functional verification test on the GuardLogix controller, you must perform a full test of the application. You must toggle each sensor and actuator involved in every safety function. From a controller perspective, this means toggling the I/O point going into the controller, not necessarily the actual activators. Be sure to test all shutdown functions, since these functions are not typically exercised during normal operation. Also, be aware that a functional verification test is only valid for the specific application tested. If the controller is moved to another application, you must also perform startup and functional verification testing on the controller in the context of its new application.

See Functional Verification Tests on page 14 for more information.

Confirm the Project

You must print or view the project, and manually compare the uploaded Safety I/O and controller configurations, safety data, and safety task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

If your application program contains a safety Add-On Instruction that has been sealed with an instruction signature, you must also compare the instruction signature, date/time, and safety instruction signature to the values you recorded when you sealed the Add-On Instruction.

See Appendix B, Safety Add-On Instructions for information on creating and using safety Add-On Instructions in SIL 3 applications.

The steps below illustrate one method for confirming the project.

1. With the controller in Program mode, save the project.
2. Answer Yes to the Upload Tag Values prompt.
3. With RSLogix 5000 software offline, save the project with a new name, such as Offlineprojectname.ACD, where projectname is the name of your project.

   This is the new tested master project file.
4. Close the project.
5. Move the original project archive file out of this directory.

   You can delete this file or store it in an archival location. This step is required because if RSLogix 5000 software finds the projectname.ACD in this directory, it will correlate it with the controller project and will not perform an actual upload.
6. With the controller still in Program mode, upload the project from the controller.
7. Save the uploaded project as Onlineprojectname.ACD, where projectname is the name of your project.
8. Answer Yes to the Upload Tag Values prompt.
9. Invoke another instance of RSLogix 5000 software and open the project named Offlineprojectname.ACD.
10. Use the two instances of RSLogix 5000 software to compare the following:
    - All of the properties of the GuardLogix controller and CIP Safety I/O modules
    - All of the properties of the safety task, safety programs and safety routines
    - All of the logic in the safety routines

TIP RSLogix 5000 software features a Program Compare utility that may be helpful in identifying changed safety components, but it must not be used in place of a manual compare. (Compare the offlineprojectname.acd to onlineprojectname.acd.)

Safety Validation

An independent, third-party review of the safety system may be required before the system is approved for operation. An independent, third-party certification is required for IEC 61508 SIL 3.

Lock the GuardLogix Controller

The GuardLogix controller system can be safety-locked to protect safety control components from modification. The safety-lock feature applies only to safety components, such as the safety task, safety programs, safety routines, safety tags, safety Add-On Instructions, safety I/O, and safety task signature. However, safety-locking alone does not satisfy SIL 3 requirements.

No aspect of safety can be modified while the controller is in the safety-locked state. When the controller is safety-locked, the following actions are not permitted in the safety task:

- Online or offline programming or editing
- Forcing safety I/O
- Data manipulation (except through routine logic or another GuardLogix controller)
- Creating or editing safety Add-On Instructions
- Generating or deleting the safety task signature

The default state of the controller is safety-unlocked. You may place the safety application in a safety-locked state regardless of whether you are online or offline, and regardless of whether you have the original source of the program. However, no safety forces or pending safety edits may be present. Safety-locked or -unlocked status cannot be modified when the keyswitch is in the RUN position.

To provide an additional layer of protection, separate passwords may be used for safety-locking or -unlocking the controller. Passwords are optional.

Downloading the Safety Application Program

Upon download, full application testing is required unless a safety task signature exists.

IMPORTANT To verify the integrity of every download, you must manually record the safety task signature after initial creation and check the safety task signature after every download to make sure that it matches the original.

Downloads to a safety-locked GuardLogix controller are allowed only if the safety task signature, the hardware series, and the OS version of the offline project all match those contained in the target GuardLogix controller and the controller's safety task status is OK.

IMPORTANT If the safety task signature does not match and the controller is safety-locked, you must unlock the controller to download. Downloading to the controller deletes the safety task signature. As a result, you must re-validate the application.

Uploading the Safety Application Program

If the GuardLogix controller contains a safety task signature, the safety task signature will be uploaded with the project. This means that any changes to offline safety data will be overwritten as a result of the upload.

Online Editing

If there is no safety task signature and the controller is safety-unlocked, you can perform online edits to your safety routines.

TIP You cannot edit standard or safety Add-On Instructions while online.

Pending edits cannot exist when the controller is safety-locked or when there is a safety task signature. Online edits may exist when the controller is safety-locked. However, they may not be assembled or cancelled.

TIP Online edits in standard routines are unaffected by the safety-locked or -unlocked state.

See page 63 for more information on making edits to your application program.

Storing and Loading a Project from Nonvolatile Memory

In version 18 or later, GuardLogix controllers support firmware upgrades and user program storage and retrieval by using a CompactFlash card. In a 1756 GuardLogix system, only the primary controller uses a CompactFlash card for nonvolatile memory.

When you store a safety application project on a CompactFlash card, Rockwell Automation recommends you select Remote Program as the Load Mode, that is, the mode the controller should enter following the load. Prior to actual machine operation, operator intervention is required to start the machine.

You can only initiate a load from nonvolatile memory:

- if the controller type specified by the project stored in nonvolatile memory matches your controller type.
- if the major and minor revisions of the project in nonvolatile memory matches the major and minor revisions of your controller.
- if your controller is not in Run mode.

Loading a project to a safety-locked controller is allowed only when the safety task signature of the project stored in nonvolatile memory matches the project on the controller. If the signatures do not match or the controller is safety-locked without a safety task signature, you must first unlock the controller before attempting to update the controller via nonvolatile memory.

IMPORTANT If you unlock the controller and initiate a load from nonvolatile memory, the safety-lock status, passwords, and safety task signature will be set to the values contained in nonvolatile memory once the load is complete.

Force Data

All data contained in an I/O, produced, or consumed safety tag, including CONNECTION_STATUS, can be forced while the project is safety-unlocked and no safety task signature exists. However, forces must be uninstalled, not just disabled, on all safety tags before the safety project can be safety-locked or a safety task signature can be generated. You cannot force safety tags while the project is safety-locked or when a safety task signature exists.

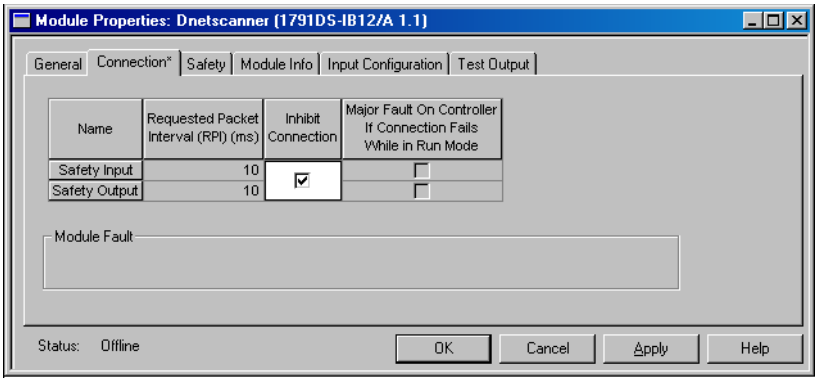
TIP You can install and uninstall forces on standard tags regardless of the safety-locked or -unlocked state.

Inhibit a Module

You cannot inhibit or uninhibit Safety I/O modules or producer controllers if the application is safety-locked or a safety task signature exists.

Follow these steps to inhibit a specific Safety I/O module.

1. In RSLogix 5000 software, right-click the module and choose Properties.
2. On the Module Properties dialog, click the Connection tab.
3. Check Inhibit Connection and click Apply.



The module is inhibited whenever the checkbox is checked. If a communication module is inhibited, all downstream modules are also inhibited.

Editing Your Safety Application

The following rules apply to changing your Safety application in RSLogix 5000 software:

- Only authorized, specially-trained personnel can make program edits. These personnel should use all supervisory methods available, for example, using the controller keyswitch and software password protections.
- When authorized, specially-trained personnel make program edits, they assume the central safety responsibility while the changes are in progress. These personnel must also maintain safe application operation.
- When editing online, you must use an alternate protection mechanism to maintain the safety of the system.
- You must sufficiently document all program edits, including:
  - authorization.
  - impact analysis.
  - execution.
  - test information.
  - revision information.

- If online edits exist only in the standard routines, those edits are not required to be validated before returning to normal operation.
- You must ensure that changes to the standard routine, with respect to timing and tag mapping, are acceptable to your safety application.
- You **can** edit the logic portion of your program while offline or online, as described in the following sections.

Performing Offline Edits

When offline edits are made to only standard program elements, and the safety task signature matches following a download, you can resume operation.

When offline edits affect the safety program, you must revalidate the entire application before resuming operation.

The flowchart on page 65 illustrates the process for offline editing.

Performing Online Edits

If online edits affect the safety program, you must revalidate the entire application before resuming operation. The flowchart on page 65 illustrates the process for online editing.

TIP Limit online edits to minor program modifications such as setpoint changes or logic additions, deletions, and modifications.

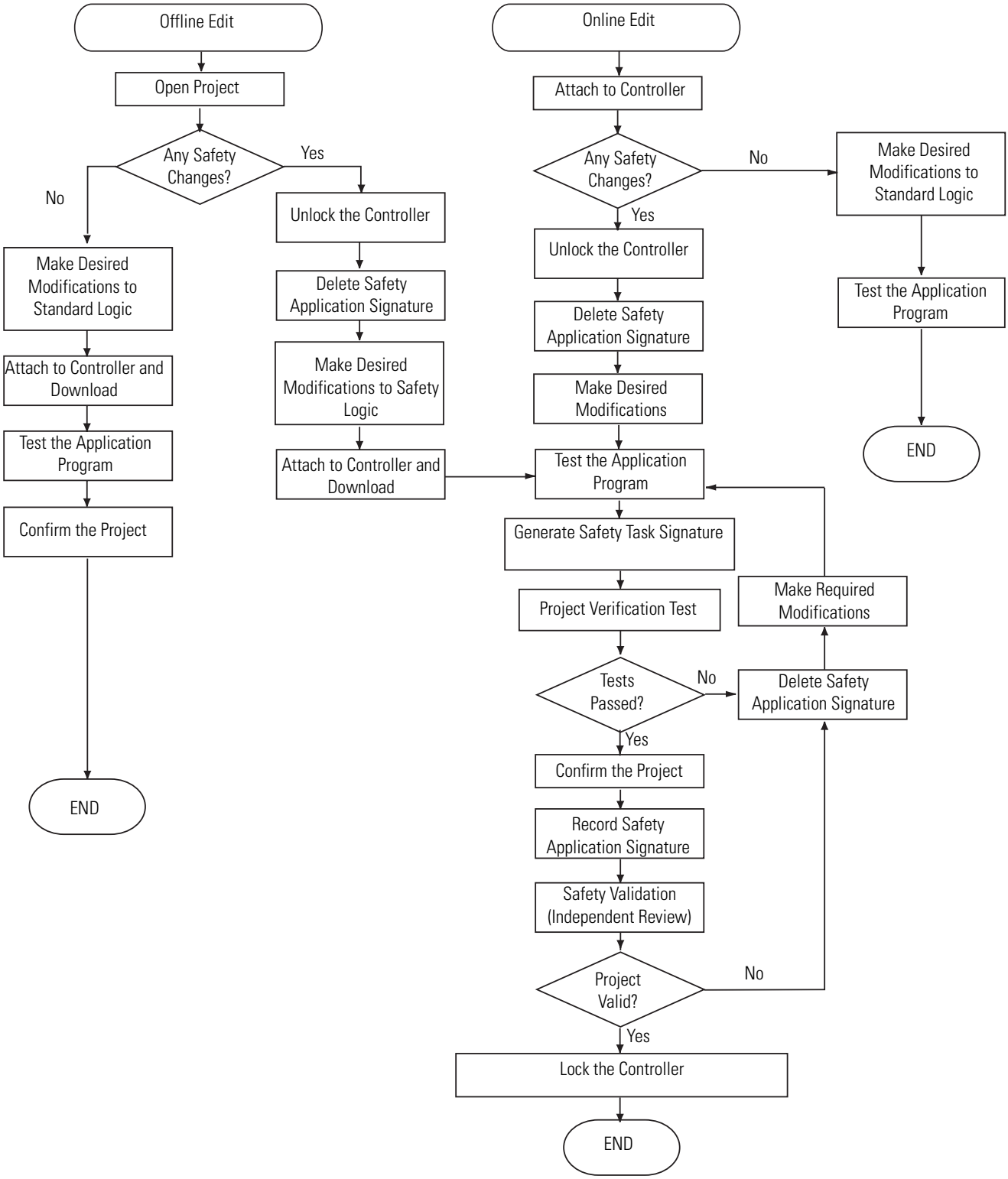
Online edits are affected by the safety-lock and safety task signature features of the GuardLogix controller.

See Generate the Safety Task Signature on page 57 and Lock the GuardLogix Controller on page 60 for more information.

For detailed information on how to edit ladder logic in RSLogix 5000 software while online, see the Logix5000 Controllers Quick Start, publication 1756-QS001.

Edit Your Project

Online and Offline Edit Process



Notes:

Monitor Status and Handle Faults

Introduction

The GuardLogix architecture provides you with many ways of detecting and reacting to faults in the system. The first way that you can handle faults is to make sure you have completed the checklists for your application (see Appendix D).

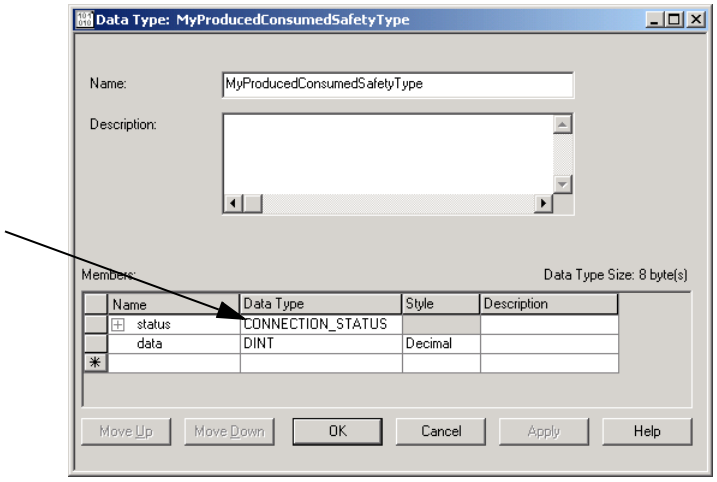
Topic	Page
Monitoring System Status	67
GuardLogix System Faults	74

Monitoring System Status

To monitor system status, you can view the status of safety tag connections. You can also determine current operating status by interrogating various device objects. It is your responsibility to determine what data is most appropriate to initiate a shutdown sequence.

CONNECTION_STATUS Data

The first member of the tag structure associated with safety input data and produced/consumed safety tag data contains the status of the connection. This member is a pre-defined data type called CONNECTION_STATUS.



The CONNECTION_STATUS data type contains RunMode and ConnectionFaulted status bits. The following table describes the combinations of the RunMode and ConnectionFaulted states.

Safety Connection Status

RunMode Status	ConnectionFaulted Status	Safety Connection Operation
1 = Run	0 = Valid	Data is actively being controlled by the producing device. The producing device is in Run mode.
0 = Idle	0 = Valid	The connection is active and the producing device is in the Idle state. The safety data is reset to zero.
0 = Idle	1 = Faulted	The safety connection is faulted. The state of the producing device is unknown. The safety data is reset to zero.
1	1	Invalid state.

ATTENTION

Safety I/O connections and produced/consumed connections cannot be configured to fault the controller if a connection is lost and the system transitions to the safe state. Therefore, if you need to detect a module fault to ensure that the system maintains SIL 3, you must monitor the Safety I/O CONNECTION_STATUS bits and initiate the fault via program logic.

Input and Output Line Conditioning

I/O modules provide pulse test and monitoring capabilities. If the module detects a failure, it sets the offending input or output to its safety state and reports the failure to the controller. The failure indication is made via input or output status and is maintained for a configurable amount of time after the failure is repaired.

IMPORTANT

You are responsible for providing application logic to latch these I/O failures and to make sure the system restarts properly.

I/O Module Connection Status

The safety protocol portion of the controller's operating system provides status for each I/O module in the safety system. If an input connection failure is detected, the operating system sets all associated

inputs to their de-energized (safety) state, and the associated input status to faulted. If an output connection failure is detected, the operating system sets the associated output status to faulted. The output module de-energizes the outputs.

IMPORTANT You are responsible for providing application logic to latch these I/O failures and to make sure the system restarts properly.

De-energize to Trip System

GuardLogix controllers are part of a de-energize to trip system, which means that zero is the safety state. All inputs and outputs are set to zero when a fault is detected. As a result, any inputs being monitored by one of the diverse input instructions (Diverse Inputs or Two-hand Run Station) should have normally-closed inputs conditioned by logic similar to the logic in Rung 4 of Ladder Logic Example 2 and Ladder Logic Example 3 on pages 72 and 73. The exact logic required is both application and input-module dependent. However, the logic must create a safety state of 1 for the normally-closed input of the diverse input instructions.

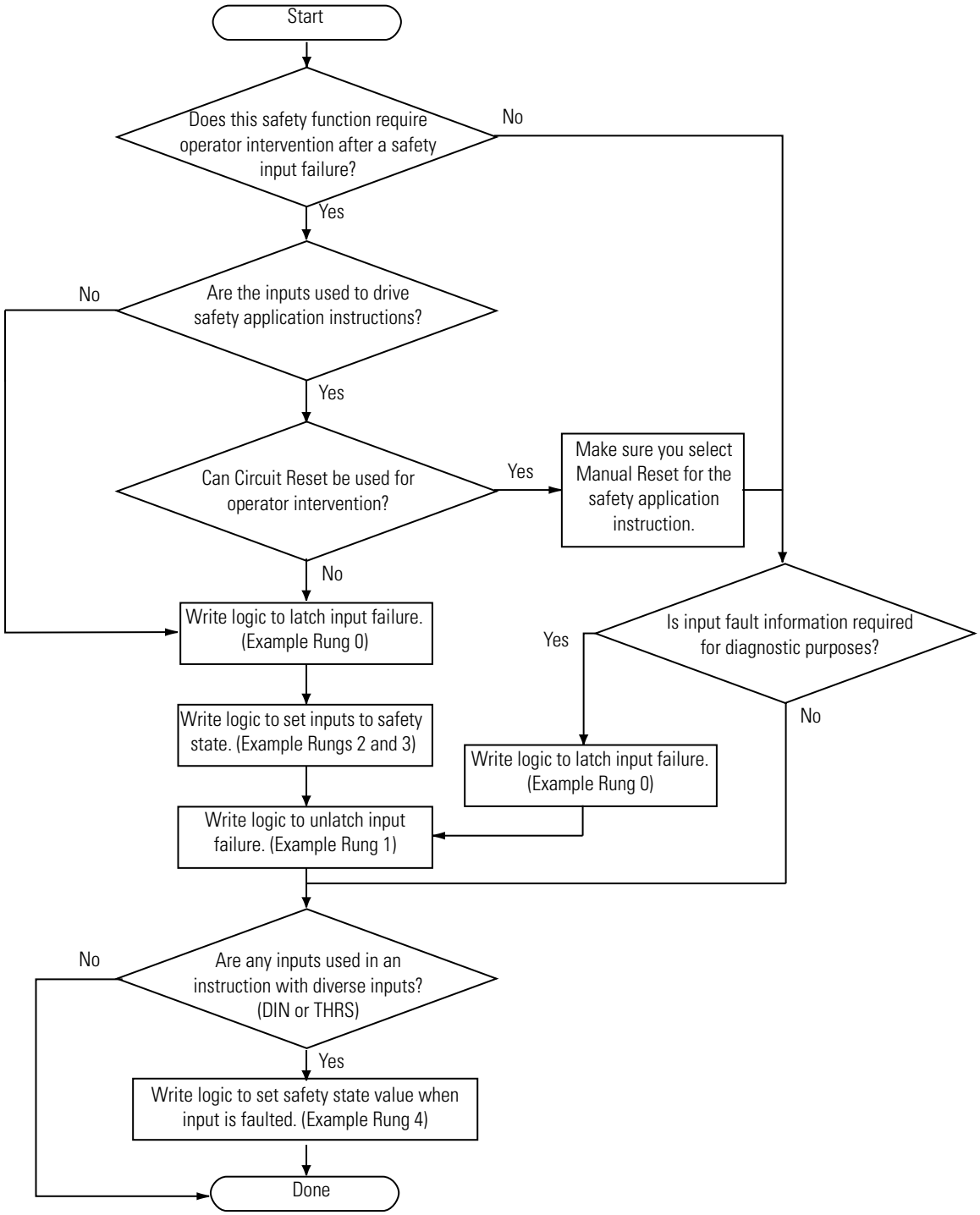
Use Connection Status Data to Initiate a Fault Via Program Logic

The following diagrams provide examples of the application logic required to latch and reset I/O failures. The examples show the logic necessary for input only modules, as well as input and output combination modules. The examples use a feature of the I/O modules called Combined Status, which presents the status of all of the input channels in a single boolean variable. Another boolean variable represents the status of all the output channels. This approach reduces the amount of I/O conditioning logic required and forces the logic to shut down all input or output channels on the affected module.

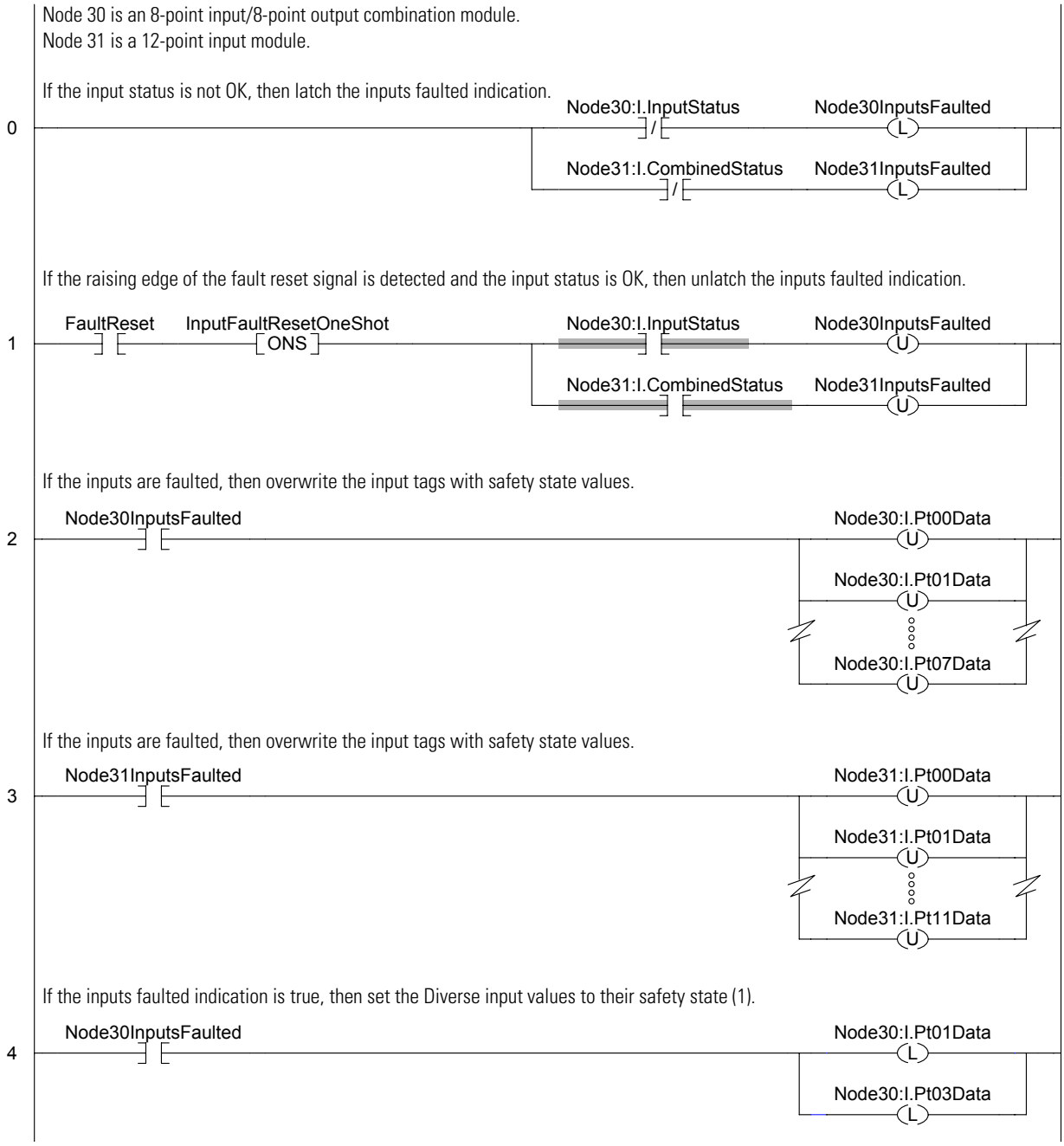
Use the Input Fault Latch and Reset Flow Chart on page 70 to determine which rungs of logic are required for different application situations. Ladder Logic Example 1 shows logic that overwrites the actual input tag variables while a fault condition exists. If the actual input state is required for troubleshooting while the input failure is latched, use the logic shown in Ladder Logic Example 2. This logic uses internal tags that represent the inputs to be used in the application logic. While the input failure is latched, the internal tags are set to their safety state. While the input failure is not latched, the actual input values are copied to the internal tags.

Use the Output Fault Latch and Reset Flowchart to determine which rungs of application logic in Ladder Logic Example 3 on page 73 are required.

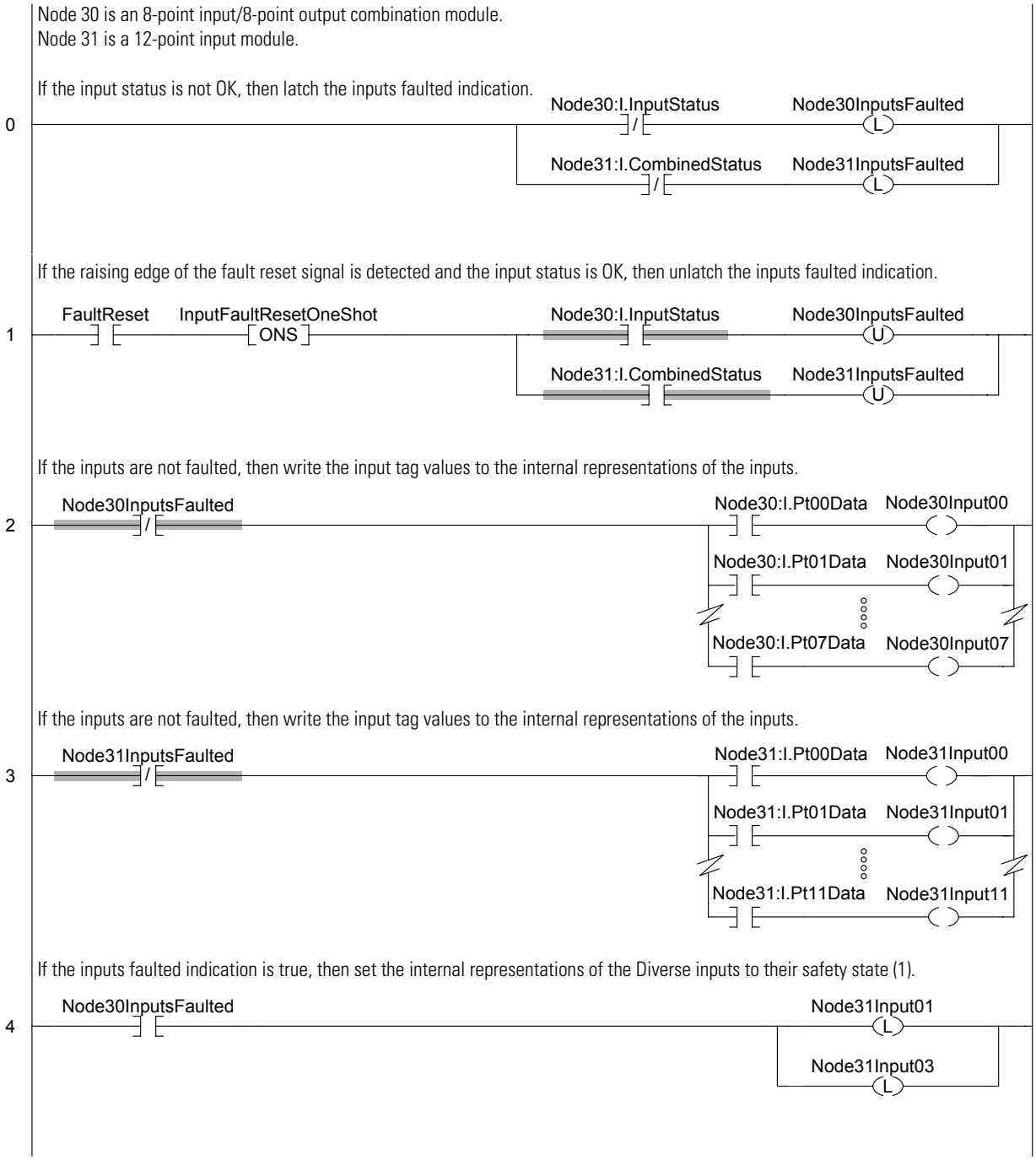
Input Fault Latch and Reset Flow Chart


Start
Does this safety function require operator intervention after a safety input failure?
No
Yes
Are the inputs used to drive safety application instructions?
No
Yes
Can Circuit Reset be used for operator intervention?
Yes
Make sure you select Manual Reset for the safety application instruction.
No
Write logic to latch input failure. (Example Rung 0)
Is input fault information required for diagnostic purposes?
Yes
No
Write logic to latch input failure. (Example Rung 0)
Write logic to set inputs to safety state. (Example Rungs 2 and 3)
Write logic to unlatch input failure. (Example Rung 1)
Are any inputs used in an instruction with diverse inputs? (DIN or THRS)
No
Yes
Write logic to set safety state value when input is faulted. (Example Rung 4)
Done

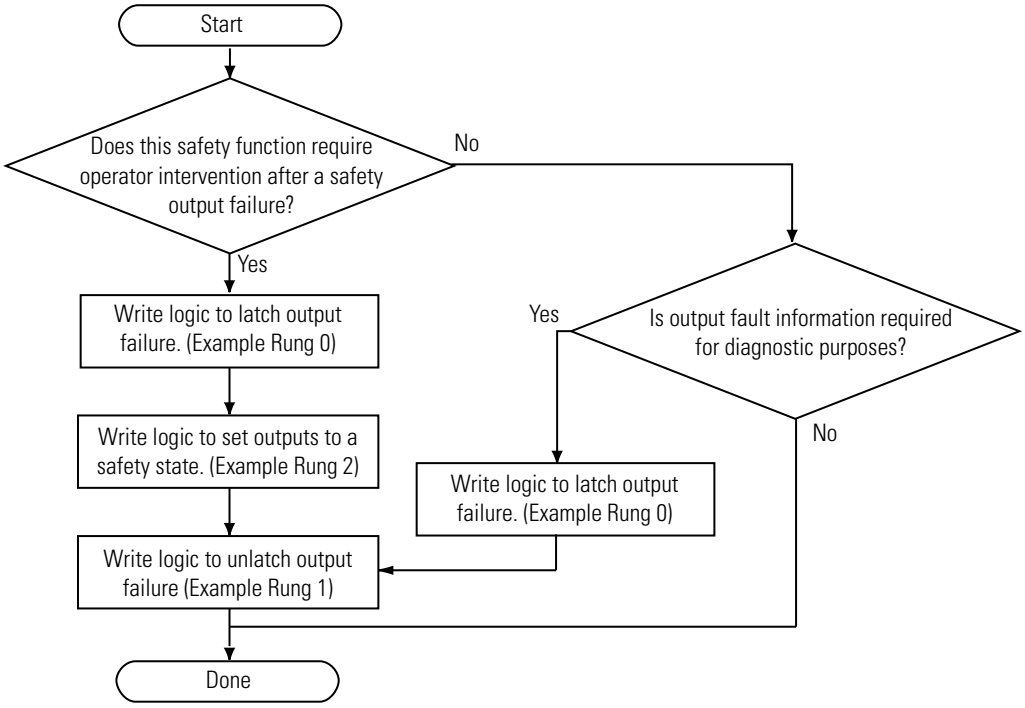
Ladder Logic Example 1



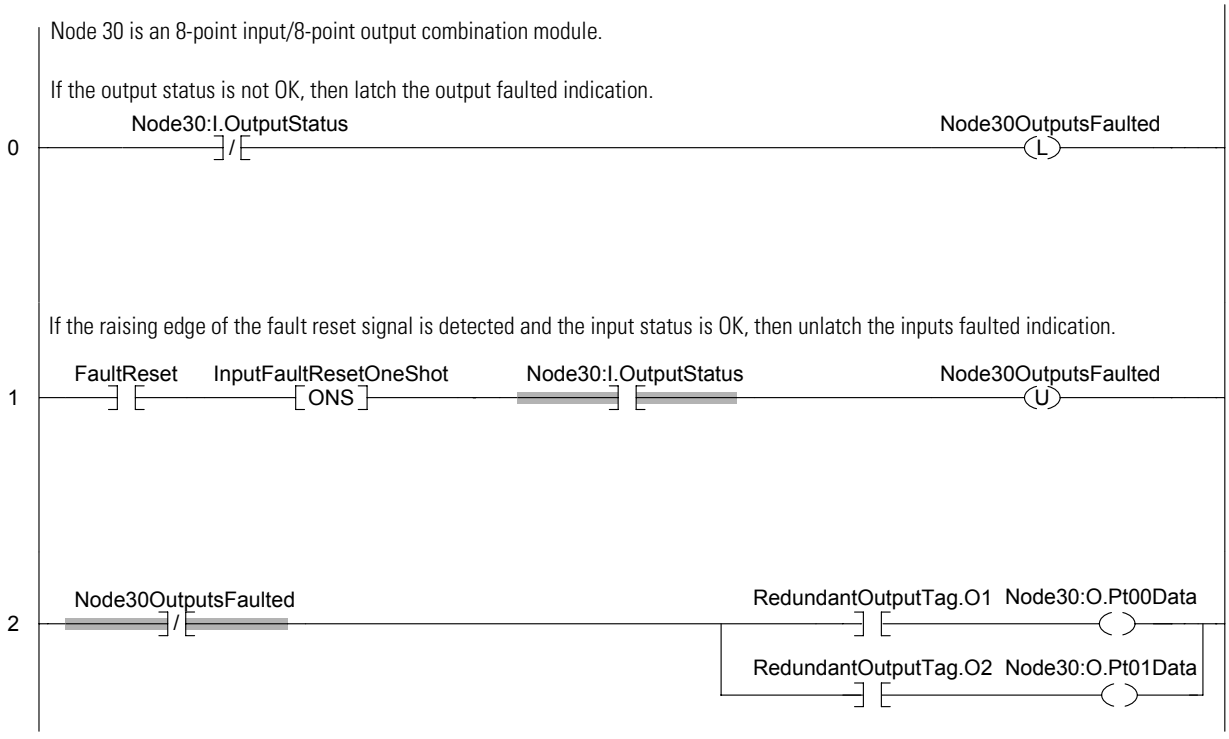
Ladder Logic Example 2



Output Fault Latch and Reset Flowchart


Start
Does this safety function require operator intervention after a safety output failure?
No
Yes
Write logic to latch output failure. (Example Rung 0)
Write logic to set outputs to a safety state. (Example Rung 2)
Write logic to unlatch output failure (Example Rung 1)
Done
Yes
Is output fault information required for diagnostic purposes?
No
Write logic to latch output failure. (Example Rung 0)

Ladder Logic Example 3



Get System Value (GSV) and Set System Value (SSV) Instructions

The GSV and SSV instructions let you get (GSV) and set (SSV) controller system data stored in device objects. When you enter a GSV/SSV instruction, the programming software displays the valid object classes, object names, and attribute names for each instruction. Restrictions exist for using the GSV and SSV instructions with safety components.

IMPORTANT The safety task cannot perform GSV or SSV operations on standard attributes.

The attributes of safety objects that can be written by the standard task are for diagnostic purposes only. They do not affect safety task execution.

Additional Resources

Resource	Description
GuardLogix Controllers User Manual, publication 1756-UM020	Provides information on which safety attributes are accessible via GSV and SSV instructions
1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002	
Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Contains more information on using GSV and SSV instructions

GuardLogix System Faults

Faults in the GuardLogix system fall into these three categories:

- Nonrecoverable controller faults
- Nonrecoverable safety faults
- Recoverable faults

For information on handling faults, refer to the GuardLogix Controllers User Manual, publication 1756-UM020, or the 1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002.

Nonrecoverable Controller Faults

A nonrecoverable controller fault occurs if the controller's internal diagnostics fail. Partnership is lost when a nonrecoverable controller fault occurs in either the primary controller or the safety partner, causing the other to generate a nonrecoverable watchdog timeout fault. Standard task and safety task execution stops, and Safety I/O transitions to the safe state.

Recovery from a nonrecoverable controller fault requires a download of the application program.

Nonrecoverable Safety Faults

In the event of a non-recoverable safety fault, the controller logs the fault to the controller-scoped fault handler and shuts down the safety task, including Safety I/O and safety logic.

To recover from a nonrecoverable safety fault, safety memory is reinitialized either from the safety task signature (happens automatically when you clear the fault) or, if no safety task signature exists, via an explicit download of the safety project.

You can override the safety fault by clearing the fault log entry through the controller-scoped safety fault handler. This allows standard tasks to keep running.

ATTENTION

Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that doing so maintains SIL 3.

Recoverable Faults

Controller faults caused by user programming errors in a safety program trigger the controller to process the logic contained in the project's safety program fault handler. The safety program fault handler provides the application with the opportunity to resolve the fault condition and then recover.

ATTENTION

You must provide proof to your certifying agency that automatic recovery from recoverable faults maintains SIL 3.

When a safety program fault handler does not exist or the fault is not recovered by it, the controller processes the logic in the controller-scoped fault handler, terminating safety program logic execution and leaving safety I/O connections active, but idle.

IMPORTANT

When the execution of safety program logic is terminated due to a recoverable fault that is not handled by the safety program fault handler, the safety I/O connections are closed and reopened to reinitialize safety connections.

If user logic is terminated as a result of a recoverable fault that is not recovered, safety outputs are placed in the safe state and the producer of safety-consumed tags commands the consumers to place them in a safe state.

TIP

When using safety I/O for standard applications, safety I/O will be commanded to the safe state if user logic is terminated as a result of a recoverable fault that is not recovered.

If a recoverable safety fault is overridden in the controller-scoped fault handler, only standard tasks keep running. If the fault is not overridden, the standard tasks are also shut down.

ATTENTION

Overriding the safety fault does not clear it. If you override the safety fault, it is your responsibility to prove that doing so maintains SIL 3.

Safety Instructions

Introduction

Topic	Page
Safety Application Instructions	77
Metal Form Safety Application Instructions	79
Safety Instructions	80
Additional Resources	81

For the latest information, see our safety certificates at http://www.rockwellautomation.com/products/certification/safety/.

Safety Application Instructions

RSLogix 5000, Version 17 and Later, Safety Application Instructions

Mnemonic	Name	Purpose	Certification
CROUT	Configurable Redundant Output	Controls and monitors redundant outputs.	• BG • TÜV
DCS	Dual Channel Input - Stop	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch.	• BG • TÜV
DCST	Dual Channel Input - Stop With Test	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability of initiating a functional test of the stop device.	• BG • TÜV
DCSTL	Dual Channel Input - Stop With Test and Lock	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability of initiating a functional test of the stop device and can monitor a feedback signal from a safety device and issue a lock request to a safety device.	• BG • TÜV
DCSTM	Dual Channel Input - Stop With Test and Mute	Monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch. It includes the added capability of initiating a functional test of the stop device and the ability to mute the safety device.	TÜV
DCM	Dual Channel Input - Monitor	Monitors dual-input safety devices.	• BG • TÜV
DCSRT	Dual Channel Input - Start	Energizes dual-input safety devices whose main function is to start a machine safely, for example an enable pendant.	• BG • TÜV
SMAT	Safety Mat	Indicates whether or not the safety mat is occupied.	TÜV

Mnemonic	Name	Purpose	Certification
THRSe	Two-Hand Run Station – Enhanced	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control a single output. Features configurable channel-to-channel discrepancy time and enhanced capability for bypassing a two-hand run station.	• BG • TÜV
TSAM	Two Sensor Asymmetrical Muting	Provides temporary, automatic disabling of the protective function of a light curtain, using two muting sensors arranged asymmetrically.	TÜV
TSSM	Two Sensor Symmetrical Muting	Provides temporary, automatic disabling of the protective function of a light curtain, using two muting sensors arranged symmetrically.	TÜV
FSBM	Four Sensor Bidirectional Muting	Provides temporary, automatic disabling of the protective function of a light curtain, using four sensors arranged sequentially before and after the light curtain's sensing field.	TÜV

RSLogix 5000, Version 14 and Later, Safety Application Instruction Descriptions

Mnemonic	Name	Purpose	Certification
ENPEN	Enable Pendant	Monitors two safety inputs to control a single output and has a 3-s inputs-inconsistent timeout value.	• TÜV
ESTOP	E-Stop	Monitors two safety inputs to control a single output and has a 500-ms inputs-inconsistent timeout value.	• TÜV
RIN	Redundant Input	Monitors two safety inputs to control a single output and has a 500-ms inputs-inconsistent timeout value.	• TÜV
ROUT	Redundant Output	Monitors the state of one input to control and monitor two outputs.	• TÜV
DIN	Diverse Input	Monitors two diverse safety inputs to control a single output and has a 500-ms inputs-inconsistent timeout value.	• TÜV
FPMS	5-Position Mode Selector	Monitors five safety inputs to control one of the five outputs corresponding to the active input.	• TÜV
THRS	Two Handed Run Station	Monitors two diverse safety inputs, one from a right-hand push button and one from a left-hand push button, to control a single output.	• TÜV
LC	Light Curtain	Monitors two safety inputs from a Light Curtain to control a single output.	• TÜV

Metal Form Safety Application Instructions

These instructions are available in RSLogix 5000 software, version 17 and later.

Mnemonic	Name	Purpose	Certification
CBCM	Clutch Brake Continuous Mode	Used for press applications where continuous operation is desired.	• BG • TÜV
CBIM	Clutch Brake Inch Mode	Used for press applications where minor slide adjustments are required, such as press setup.	• BG • TÜV
CBSSM	Clutch Brake Single Stoke Mode	Used in single-cycle press applications.	• BG • TÜV
CPM	Crankshaft Position Monitor	Used to determine the slide position of the press.	• BG • TÜV
CSM	Camshaft Monitor	Monitors motion for the starting, stopping, and running operations of a camshaft.	• BG • TÜV
EPMS	Eight-position Mode Selector	Monitors eight safety inputs to control one of the eight outputs corresponding to the active input.	• BG • TÜV
AVC	Auxiliary Valve Control	Controls an auxiliary valve that is used in conjunction with a main valve.	• TÜV
MVC	Main Valve Control	Controls and monitors a main valve.	• BG • TÜV
MMVC	Maintenance Manual Valve Control	Used to manually drive a valve during maintenance operations.	• BG • TÜV

Safety Instructions

Routines in the safety task may use these ladder logic safety instructions.

Ladder Logic Safety Instructions, RSLogix 5000 Software, Version 14 and Later

Type	Mnemonic	Name	Purpose
Bit	XIC	Examine If Closed	Enable outputs when a bit is set
	XIO	Examine If Open	Enable outputs when a bit is cleared
	OTE	Output Energize	Set a bit
	OTL	Output Latch	Set a bit (retentive)
	OTU	Output Unlatch	Clear bit (retentive)
	ONS	One Shot	Triggers an event to occur one time
	OSR	One Shot Rising	Triggers an event to occur one time on the false-to-true (rising) edge of change-of-state
	OSF	One Shot Falling	Triggers an event to occur one time on the true-to-false (falling) edge of change-of-state
Timer	TON	Timer On Delay	Time how long a timer is enabled
	TOF	Timer Off Delay	Time how long a timer is disabled
	RTO	Retentive Timer On	Accumulate time
	CTU	Count Up	Count up
	CTD	Count Down	Count down
	RES	Reset	Reset a timer or counter
Compare	EQU	Equal To	Test whether two values are equal
	GEQ	Greater Than Or Equal To	Test whether one value is greater than or equal to a second value
	GRT	Greater Than	Test whether one value is greater than a second value
	LEQ	Less Than Or Equal To	Test whether one value is less than or equal to a second value
	LES	Less Than	Test whether one value is less than a second value
	MEQ	Masked Comparison for Equal	Pass source and compare values through a mask and test whether they are equal
	NEQ	Not Equal To	Test whether one value is not equal to a second value
	LIM	Limit Test	Test whether a value falls within a specified range
Move	CLR	Clear	Clear a value
	COP[1]	Copy	Copy a value
	MOV	Move	Copy a value
	MVM	Masked Move	Copy a specific part of an integer
Logical	AND	Bitwise AND	Perform bitwise AND operation
	NOT	Bitwise NOT	Perform bitwise NOT operation
	OR	Bitwise OR	Perform bitwise OR operation
	XOR	Bitwise Exclusive OR	Perform bitwise exclusive OR operation

Ladder Logic Safety Instructions, RSLogix 5000 Software, Version 14 and Later

Type	Mnemonic	Name	Purpose
Program Control	JMP	Jump To Label	Jump over a section of logic that does not always need to be executed (skips to referenced label instruction)
	LBL	Label	Labels an instruction so that it can be referenced by a JMP instruction
	JSR	Jump to Subroutine	Jump to a separate routine
	RET	Return	Return the results of a subroutine
	SBR	Subroutine	Pass data to a subroutine
	TND	Temporary End	Mark a temporary end that halts routine execution
	MCR	Master Control Reset	Disable all the rungs in a section of logic
	AFI	Always False Instruction	Disable a rung
	NOP	No Operation	Insert a placeholder in the logic
Math/ Compute	ADD	Add	Add two values
	SUB	Subtract	Subtract two values
	MUL	Multiply	Multiply two values
	DIV	Divide	Divide two values
	MOD	Modulo	Determine the remainder after one value is divided by a second value
	SQR	Square Root	Calculate the square root of a value
	NEG	Negate	Take the opposite sign of a value
	ABS	Absolute Value	Take the absolute value of a value
I/O	GSV(2)	Get System Value	Get controller status information
	SSV(2)	Set System Value	Set controller status information

(1) The length operand must be a constant when the COP instruction is used in a safety routine. The length of the source and the destination must be the same.
(2) Refer to the GuardLogix Controllers User Manual, publication 1756-UM020, for special considerations when using the GSV and SSV instructions.

Additional Resources

Resource	Description
GuardLogix Safety Application Instruction Set Reference Manual, publication 1756-RM095	Provides more information on the safety application instructions
Logix5000 Controllers General Instructions Reference Manual, publication 1756-RM003	Contains detailed information on the Logix instruction set

Safety Add-On Instructions

Introduction

Topic	Page
Creating and Using a Safety Add-On Instruction	83
Additional Resources	88

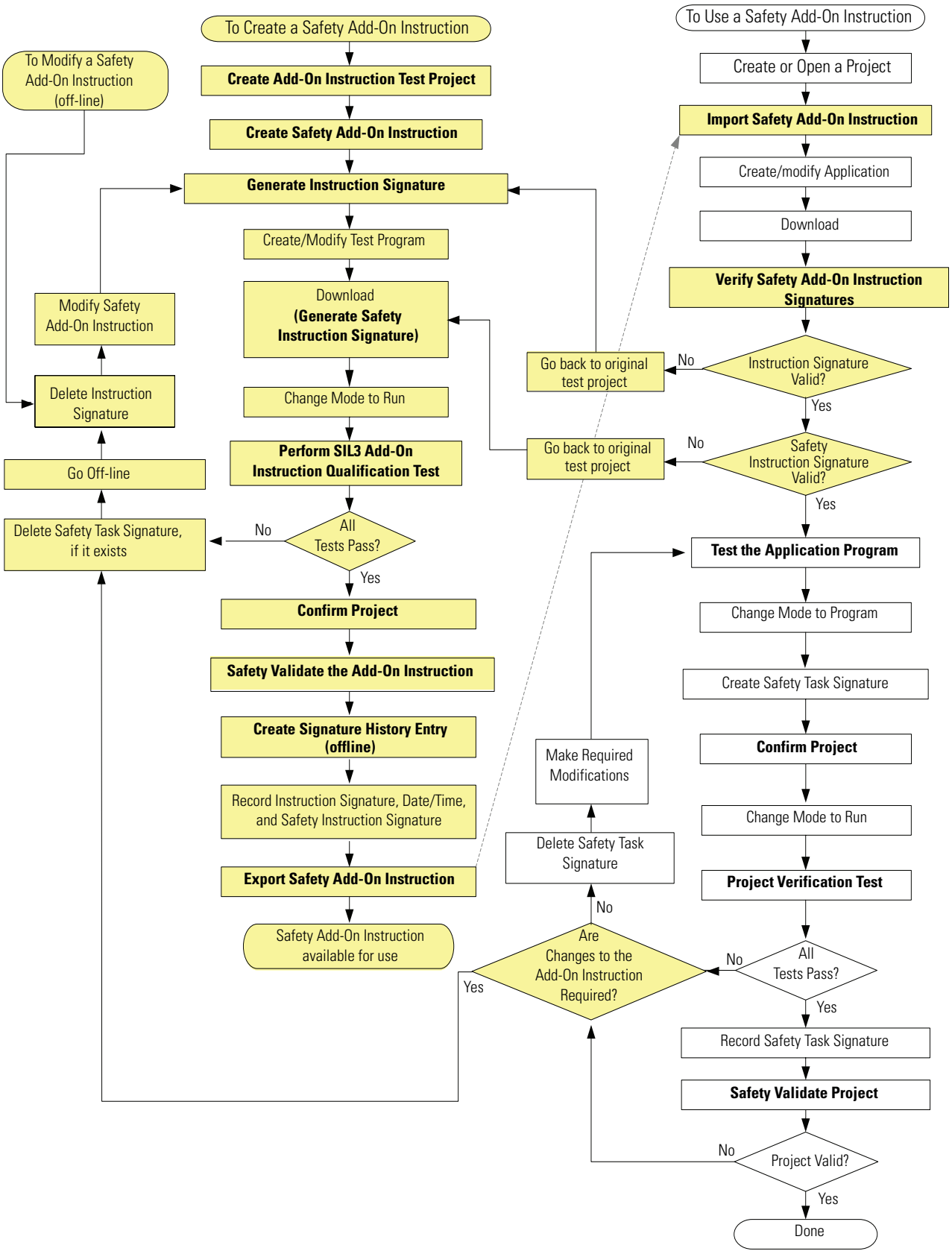
With RSLogix 5000 software, version 18 and later, you can create safety Add-On Instructions. Safety Add-On Instructions let you encapsulate commonly-used safety logic into a single instruction, making it modular and easier to reuse.

Safety Add-On Instructions use the instruction signature of high-integrity Add-On Instructions and also a SIL 3 safety instruction signature for use in safety-related functions up to and including SIL 3.

Creating and Using a Safety Add-On Instruction

The flowchart on page 84 shows the steps required for creating a safety Add-On Instruction and then using that instruction in a SIL 3 safety application program. The shaded items are steps unique to Add-On Instructions. The items in bold text are explained in the pages following the flowchart.

Flowchart for Creating and Using Safety Add-On Instructions


To Create a Safety Add-On Instruction
Create Add-On Instruction Test Project
Create Safety Add-On Instruction
Generate Instruction Signature
Create/Modify Test Program
Download (Generate Safety Instruction Signature)
Change Mode to Run
Perform SIL3 Add-On Instruction Qualification Test
All Tests Pass?
No
Yes
Confirm Project
Safety Validate the Add-On Instruction
Create Signature History Entry (offline)
Record Instruction Signature, Date/Time, and Safety Instruction Signature
Export Safety Add-On Instruction
Safety Add-On Instruction available for use
To Modify a Safety Add-On Instruction (off-line)
Modify Safety Add-On Instruction
Delete Instruction Signature
Go Off-line
Delete Safety Task Signature, if it exists
To Use a Safety Add-On Instruction
Create or Open a Project
Import Safety Add-On Instruction
Create/modify Application
Download
Verify Safety Add-On Instruction Signatures
Instruction Signature Valid?
Go back to original test project
Safety Instruction Signature Valid?
Go back to original test project
Test the Application Program
Change Mode to Program
Create Safety Task Signature
Confirm Project
Change Mode to Run
Project Verification Test
All Tests Pass?
Are Changes to the Add-On Instruction Required?
Make Required Modifications
Delete Safety Task Signature
Record Safety Task Signature
Safety Validate Project
Project Valid?
Done

Create Add-On Instruction Test Project

You need to create a unique test project, specifically for creating and testing the safety Add-On Instruction. This must be a separate and dedicated project to minimize any unexpected influences.

Follow the guidelines for projects described in Create the Project on page 56.

Create a Safety Add-On Instruction

For guidance in creating Add-On Instructions, refer to the Logix5000 Controllers Add-On Instruction Programming Manual, publication 1756-PM010.

Generate Instruction Signature

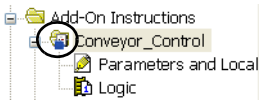
The instruction signature lets you quickly determine if the instruction has been modified. Each Add-On Instruction has the ability to have its own signature. The instruction signature is required when an Add-On Instruction is used in safety-related functions, and may be required for regulated industries. Use it when your application calls for a higher level of integrity.

The instruction signature consists of an ID number and timestamp that identifies the contents of the Add-On Instruction at a given point in time.

Once generated, the instruction signature seals the Add-On Instruction, preventing it from being edited while the signature is in place. This includes rung comments, tag descriptions, and any instruction documentation that was created. When the instruction is sealed, you can perform only these actions:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

When an instruction signature has been generated, RSLogix 5000 software displays the instruction definition with the seal icon.



IMPORTANT If you plan to protect your Add-On Instruction by using the source protection feature in RSLogix 5000 software, you must enable source protection prior to generating the instruction signature.

Download and Generate Safety Instruction Signature

When a sealed safety Add-On Instruction is downloaded for the first time, a SIL 3 safety instruction signature is automatically generated. The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction.

SIL 3 Add-On Instruction Qualification Test

Safety Add-On Instruction SIL 3 tests must be performed in a separate, dedicated application to make sure unintended influences are minimized. The developer must follow a well-designed test plan and perform a unit test of the safety Add-On Instruction that exercises all possible execution paths through the logic, including the valid and invalid ranges of all input parameters.

Development of all safety Add-On Instructions must meet IEC 61508 - 'Requirements for software module testing', which provides detailed requirements for unit testing.

Confirm the Project

You must print or view the project, and manually compare the uploaded safety I/O and controller configurations, safety data, safety Add-On Instruction definitions, and safety task program logic to make sure that the correct safety components were downloaded, tested, and retained in the safety application program.

See Confirm the Project on page 58 for a description of one method for confirming a project.

Safety Validate Add-On Instructions

An independent, third-party review of the safety Add-On Instruction may be required before the instruction is approved for use. An independent, third-party validation is required for IEC 61508 SIL 3.

Create Signature History Entry

The signature history provides a record for future reference. A signature history entry consists of the instruction signature, the name of the user, the timestamp value, and a user-defined description. Up to six history entries may be stored. You must be offline to create a signature history entry.

TIP The Signature Listing report in RSLogix 5000 software prints the instruction signature, the timestamp, and the safety instruction signature. Print the report by right-clicking Add-On Instruction in the Controller Organizer and choosing Print>Signature Listing.

Export and Import the Safety Add-On Instruction

When you export a safety Add-On Instruction, choose the option to include all referenced Add-On Instructions and User-Defined Types in the same export file. By including referenced Add-On Instructions, you make it easier to preserve the signatures.

When importing Add-On Instructions, consider these guidelines.

- You cannot import a safety Add-On Instruction into a standard project.
- You cannot import a safety Add-On Instruction into a safety project that has been safety-locked or one that has a safety task signature.
- You cannot import a safety Add-On Instruction while online.
- If you import an Add-On Instruction with an instruction signature into a project where referenced Add-On Instructions or User-Defined Types are not available, you may need to remove the signature.

Verify Safety Add-On Instruction Signatures

After you download the application project containing the imported safety Add-On Instruction, you must compare the instruction signature value, the date and timestamp, and the safety instruction signature values with the original values you recorded prior to exporting the safety Add-On Instruction. If they match, the safety Add-On Instruction is valid and you can continue with the validation of your application.

Test the Application Program

This step consists of any combination of Run and Program mode, online or offline program edits, upload and download, and informal testing that is required to get an application running properly.

Project Verification Test

Perform an engineering test of the application, including the safety system.

See Functional Verification Tests on page 14 and Project Verification Test on page 57 for more information on requirements.

Safety Validate Project

An independent, third-party review of the safety system may be required before the system is approved for operation. An independent, third-party validation is required for IEC 61508 SIL 3.

Additional Resources

Resource	Description
Logix5000 Controllers Add-On Instructions Programming Manual, publication 1756-PM010	Provides information on planning, creating, using, importing and exporting Add-On Instructions in RSLogix 5000 applications
Import/Export Project Components Programming Manual, publication 1756-PM019	Contains detailed information on importing and exporting

Reaction Times

Introduction

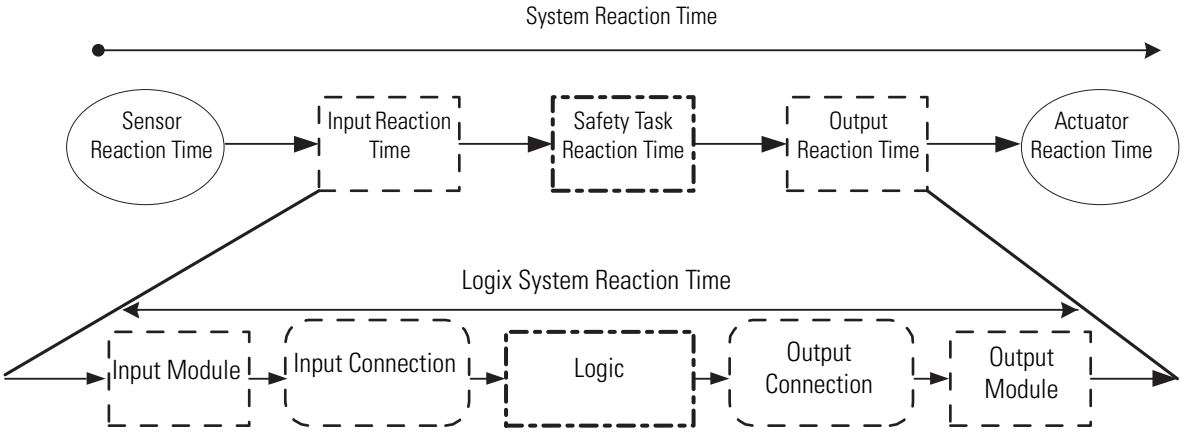
Topic	Page
System Reaction Time	89
Logix System Reaction Time	89

System Reaction Time

To determine the system reaction time of any control chain, you must add up the reaction times of all of components of the safety chain.

System Reaction Time = Sensor Reaction Time + Logix System Reaction Time + Actuator Reaction Time

System Reaction Time

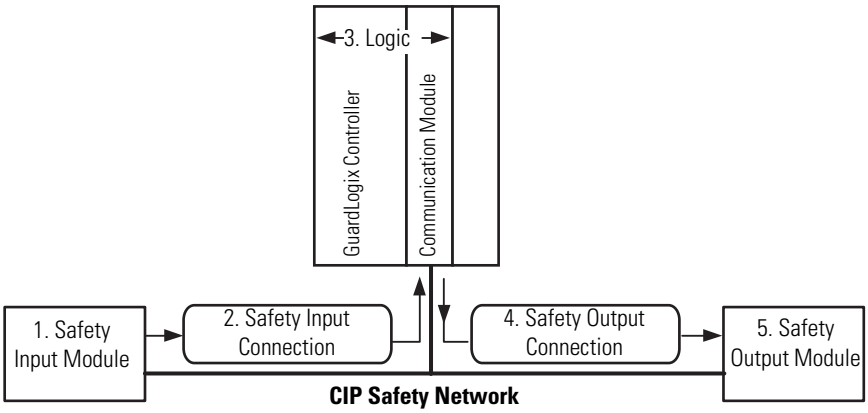


Logix System Reaction Time

The following sections provide information on calculating the Logix System Reaction Time for a simple input-logic-output chain and for a more complex application using produced/consumed safety tags in the logic chain.

Simple Input-logic-output Chain

Logix System Reaction Time for Simple Input-logic-output Chain



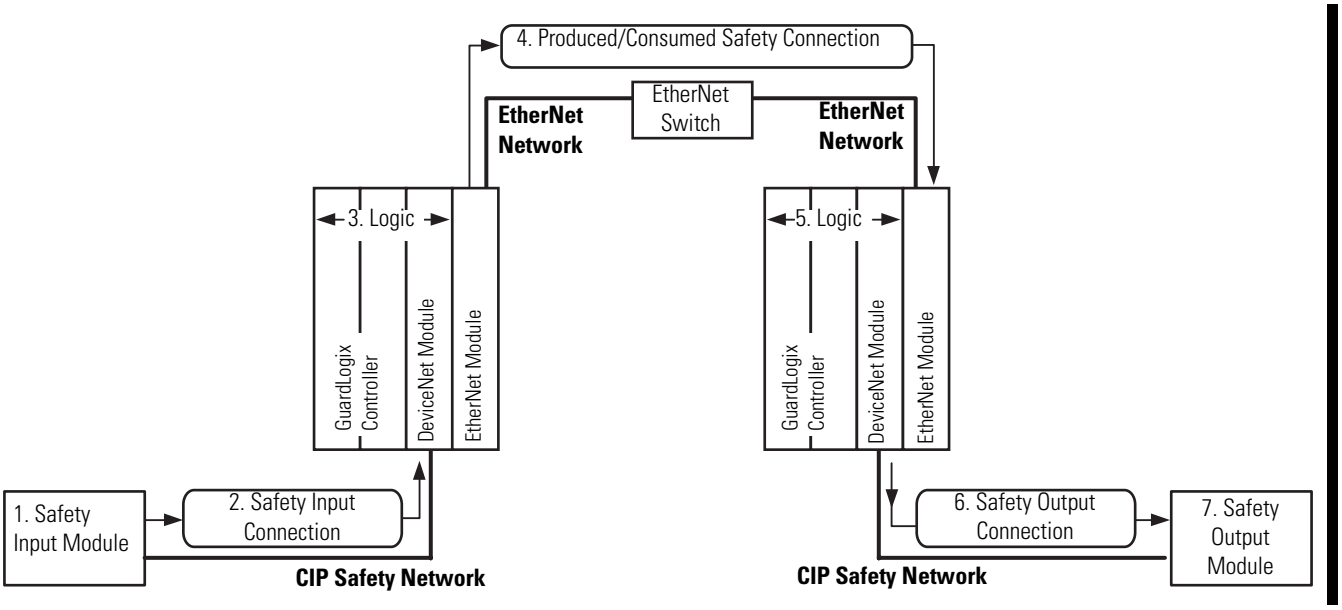
The Logix System Reaction Time for any simple input-logic-output chain consists of the following five components:

1. Input module delay time
2. Input data transfer time via the input connection
3. Controller processing time (Logic)
4. Output data transfer time via the output connection
5. Output module delay time

To aid you in determining the reaction time of your particular control loop, a Microsoft Excel spreadsheet is available in the Tools folder of the RSLogix 5000 software CD.

Logic Chain Using Produced/Consumed Safety Tags

Logix System Reaction Time for Input-Controller A Logic-Controller B Logic-Output Chain



The Logix System Reaction Time for any input-controller A logic-controller B logic-output chain consists of the following seven components:

1. Input module delay time
2. Input data transfer time via the input connection
3. Controller processing time (Logic)
4. Produced/Consumed data transfer time via the produced/consumed connection
5. Controller processing time (Logic)
6. Output data transfer time via the output connection
7. Output module delay time

To aid you in determining the reaction time of your particular control loop, a Microsoft Excel spreadsheet is available in the Tools folder of the RSLogix 5000 software CD.

Factors Affecting Logix Reaction-time Components

The Logix Reaction Time components described in the previous sections can be influenced by a number of factors.

Factors Affecting Logix System Reaction-time

These reaction time components	Are influenced by the following factors
Input module delay time	Input point delay settings
	Type of input module
Input data transfer time via the input connection	Input module settings for:(1) • RPI • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The system's EMC environment
Controller processing time	Safety Task Period setting
	Safety Task Watchdog setting
	The number and execution time of instructions in the safety task
	Any higher priority tasks that may preempt safety task execution
Produced/Consumed tag data transfer time via the produced/consumed connection	Consumed tag settings for:(2) • RPI • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The system's EMC environment
Output data transfer time via the output connection	Safety Task Period setting
	Output module's settings for: • Timeout Multiplier • Delay Multiplier
	The amount of network communication traffic
	The system's EMC environment
Output module delay time	Type of output module

(1) These settings are available in RSLogix 5000 software by pressing the Advanced button on the Safety tab of the Module Properties dialog.

(2) These settings are available in RSLogix 5000 software by pressing the Advanced button on the Safety tab of the Consumed Tag Safety Data dialog.

Additional Resources

Resource	Description
GuardLogix Controllers User Manual, publication 1756-UM020	Contains information on configuring delay times and reaction time limits for the input connection, safety task, and output connection
1768 Compact GuardLogix Controllers User Manual, publication 1768-UM002	
Consult the product documentation for your specific module for reaction times associated with CIP Safety I/O modules.	

Checklists for GuardLogix Safety Applications

Introduction

The checklists in this appendix are required for planning, programming, and start up of a SIL 3-certified GuardLogix application. They may be used as planning guides as well as during functional verification testing. If used as planning guides, the checklists can be saved as a record of the plan.

The checklists on the following pages provide a sample of safety considerations and are not intended to be a complete list of items to verify. Your particular safety application may have additional safety requirements, for which we have provided space in the checklists.

Topic	Page
Checklist for GuardLogix Controller System	96
Checklist for Safety Inputs	97
Checklist for Safety Outputs	98
Checklist for Developing a Safety Application Program	99

TIP Make copies of the checklists and keep these pages for future use.

Checklist for GuardLogix Controller System

Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
Number	**System Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using only the components listed in SIL 3-Certified GuardLogix Components on page 16 and on the http://www.rockwellautomation.com/products/certification/safety/ site, with the corresponding firmware release?	☐	☐	
2	Have you calculated the system's safety response time for each safety chain?	☐	☐	
3	Does the system's response time include both the user-defined safety task program watchdog (software watchdog) time and the safety task rate/period?	☐	☐	
4	Is the system response time in proper relation to the process tolerance time?	☐	☐	
5	Have probability (PFD/PFH) values been calculated according to the system's configuration?	☐	☐	
6	Have you performed all appropriate functional verification tests?	☐	☐	
7	Have you determined how your system will handle faults?	☐	☐	
8	Does each network in the safety system have a unique SNN?	☐	☐	
9	Is each CIP safety device configured with the correct SNN?	☐	☐	
10	Have you generated a safety task signature?	☐	☐	
11	Have you uploaded and recorded the safety task signature for future comparison?	☐	☐	
12	Following a download, have you verified that the safety task signature in the controller matches the recorded safety task signature?	☐	☐	
13	Do you have an alternate mechanism in place to preserve the safety integrity of the system when making online edits?	☐	☐	
14	Have you taken into consideration the checklists for using SIL inputs and outputs listed on pages 97 and 98?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Checklist for Safety Inputs

For programming or start up, an individual checklist can be filled in for every single SIL input channel in a system. This is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Input Checklist for GuardLogix System

Company	
Site	
Safety Function Definition	
SIL Input Channels	

Number	Input Module Requirements	Fulfilled		Comment
		Yes	No	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed functional verification tests on the system and modules?	☐	☐	
3	Are control, diagnostics, and alarming functions performed in sequence in application logic?	☐	☐	
4	Have you uploaded and compared the configuration of each module to the configuration sent by configuration tool?	☐	☐	
5	Are modules wired in compliance with PLe/Cat. 4 according to ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the sensor and input are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on wiring your CIP Safety I/O module, refer to the product documentation for your specific module.

Checklist for Safety Outputs

For programming or start up, an individual requirement checklist must be filled in for every single SIL output channel in a system. This is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Output Checklist for GuardLogix System				
Company				
Site				
Safety Function Definition				
SIL Output Channels				
Number	**Output Module Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
2	Have you performed functional verification tests on the modules?	☐	☐	
3	Have you uploaded and compared the configuration of each module to the configuration sent by configuration tool?	☐	☐	
4	Have you verified that test outputs are not used as safety outputs?	☐	☐	
5	Are modules wired in compliance with PLe/Cat. 4 according to ISO 13849-1?(1)	☐	☐	
6	Have you verified that the electrical specifications of the output and the actuator are compatible?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) For information on wiring your CIP Safety I/O module, refer to the product documentation for your specific module.

Checklist for Developing a Safety Application Program

Use the following checklist to help maintain safety when creating or modifying a safety application program.

Checklist for GuardLogix Application Program Development				
Company				
Site				
Project Definition				
Number	**Application Program Requirements**	**Fulfilled**		**Comment**
		Yes	**No**	
1	Are you using version 14, or version 16 or later of RSLogix 5000 software(1), the GuardLogix system programming software?	☐	☐	
2	Were the programming guidelines in Chapter 6 followed during creation of the safety application program?	☐	☐	
3	Does the safety application program contain only relay ladder logic?	☐	☐	
4	Does the safety application program contain only those instructions listed in Appendix A as suitable for safety application programming?	☐	☐	
5	Does the safety application program clearly differentiate between safety and standard tags?	☐	☐	
6	Are only safety tags used for safety routines?	☐	☐	
7	Have you verified that safety routines do not attempt to read from or write to standard tags?	☐	☐	
8	Have you verified that no safety tags are aliased to standard tags and vice versa?	☐	☐	
9	Is each safety output tag correctly configured and connected to a physical output channel?	☐	☐	
10	Have you verified that all mapped tags have been conditioned in safety application logic?	☐	☐	
11	Have you defined the process parameters that are monitored by fault routines?	☐	☐	
12	Have you sealed any safety Add-On Instructions with a instruction signature and recorded the safety instruction signature?	☐	☐	
13	Has the program been reviewed by an independent safety reviewer (if required)?	☐	☐	
14	Has the review been documented and signed?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) RSLogix 5000 software, version 18 or later supports 1768 Compact GuardLogix controllers.

Notes:

Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH) Data

Introduction

Topic	Page
GuardLogix Controller and Guard I/O Safety Data	101
PFD Values	102
PFH Values	102

The following examples show probability of failure on demand (PFD) and probability of failure per hour (PFH) values for GuardLogix 1oo2 SIL 3 systems.

GuardLogix Controller and Guard I/O Safety Data

All of the examples use the following data.

GuardLogix Controller Safety Specifications

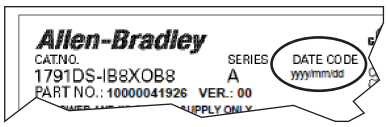
Attribute	1756 GuardLogix Controllers	1768 Compact GuardLogix Controllers
Hardware fault tolerance	1	1
Safe failure fraction	99.1%	99.0%
Functional test interval (T1)	20 years	20 years

PFD Values

Calculated PFD by Functional Test Interval

Cat. No.	Description	Calculated PFD			
		2 Years (17,520 hours)	5 Years (43,800 hours)	10 Years (87,600 hours)	20 Years (175,200 hours)
1756-L6xS and 1756-LSP	GuardLogix Controller	Not applicable		5.5E-06	1.2E-05
1768-L43S and 1768-L45S	Compact GuardLogix Controller	1.1E-06	2.7E-06	5.7E-06	1.2E-05
1791DS-IB12	CIP Safety 12-point input module	1.754E-06	4.419E-06	8.962E-06	6.013E-06(1)
1791DS-IB16	CIP Safety 16-point input module	1.70E-06	4.25E-06	8.50E-06	1.70E-05
1791DS-IB8XOB8	CIP Safety 8-point input/ 8-point output module	1.755E-06	4.421E-06	8.963E-06	6.013E-06(1)
1791DS-IB4XOW4	CIP Safety 4-point input/4-point relay output module	4.151E-05	1.207E-04	2.978E-04	7.684E-04(1)
1791DS-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	1.75E-06	4.37E-06	8.74E-06	1.75E-05
1732DS-IB8XOBV4					
1732DS-IB8	CIP Safety 8-point input module	1.70E-06	4.25E-06	8.50E-06	1.70E-05
1791ES-IB16	CIP Safety 16-point input module	1.65E-06	4.14E-06	8.27E-06	1.65E-05
1791ES-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	1.70E-06	4.26E-06	8.51E-06	1.70E-05
1734-IB8S	CIP Safety 8-point input module	1.17E-06	2.93E-06	5.86E-06	1.17E-05
1734-OB8S	CIP Safety 8-point output module	1.21E-06	3.03E-06	6.06E-06	1.21E-05

(1) The 20-year PFD data for this product applies only to product with a manufacture date code of 2009/01/01 (January 1, 2009) or later. See the product label for the date code.



PFH Values

The data below applies to proof test intervals up to and including 20 years.

PFH Calculations

Cat. No.	Description	PFH (1/Hour)
1756-L6xS and 1756-LSP	GuardLogix controller	2.0E-10
1768-L43S and 1768-L45S	Compact GuardLogix controller	2.0E-10
1791DS-IB12	CIP Safety 12-point input module	6.84E-11(1)
1791DS-IB16	CIP Safety 16-point input module	1.94E-10
1791DS-IB8XOB8	CIP Safety 8-point input/ 8-point output module	6.84E-11(1)
1791DS-IB4XOW4	CIP Safety 4-point input/4-point relay output module	4.072E-09(1)
1791DS-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	2.00E-10
1732DS-IB8XOBV4		
1732DS-IB8	CIP Safety 8-point input module	1.94E-10
1791ES-IB16	CIP Safety 16-point input module	1.89E-10
1791ES-IB8XOBV4	CIP Safety 8-point input/4 bi-polar output module	1.94E-10
1734-IB8S	CIP Safety 8-point input module	1.34E-10
1734-OB8S	CIP Safety 8-point output module	1.38E-10

(1) The PFH data for this product applies only to product with a manufacture date code of 2009/01/01 (January 1, 2009) or later. See the product label for the date code.

Add-On Instruction

An instruction that you create as an add-on to the Logix instruction set. Once defined, an Add-On Instruction can be used like any other Logix instruction and can be used across various projects. An Add-On Instruction is composed of parameters, local tags, logic routine, and optional scan mode routines.

Assemble Edits

You assemble edits when you have made online edit changes to the controller program and want the changes to become permanent since you can test, un-test, or cancel the edits.

Cancel Edits

Action taken to reject any unassembled online edit changes.

CIP Safety Protocol

A network communication method designed and certified for transport of data with high integrity.

Configuration Signature

A unique number that identifies a device's configuration. The configuration signature is made up of an ID number, date, and time.\

Instruction Signature

The instruction signature consists of an ID number, and date/timestamp that identifies the contents of the Add-On Instruction definition at a given point in time.

Nonrecoverable Controller Fault

A fault that forces all processing to be terminated and requires controller power to be cycled from off to on. The user program is not preserved and must be redownloaded.

Nonrecoverable Safety Fault

A fault, which even though properly handled by the fault handling mechanisms provided by the safety controller and implemented by the user, terminates all safety task processing, and requires external user action to restart the safety task.

Online

Situation where you are monitoring/modifying the program in the controller.

Overlap

When a task (periodic or event) is triggered while the task is still executing from the previous trigger.

Partnership

The primary controller and safety partner must both be present, and the hardware and firmware must be compatible for partnership to be established.

Pending Edit

A change to a routine that has been made in RSLogix 5000 software, but has not yet been communicated to the controller by accepting the edit.

Periodic Task

A task that is triggered by the operating system at a repetitive period of time. Whenever the time expires, the task is triggered and its programs are executed. Data and outputs established by the programs in the task retain their values until the next execution of the task or until they are manipulated by another task. Periodic tasks always interrupt the continuous task.

Primary Controller

The processor in a dual-processor controller that performs standard controller functionality and communicates with the safety partner to perform safety-related functions.

Recoverable Fault

A fault, which when properly handled by implementing the fault handling mechanisms provided by the controller, does not force user logic execution to be terminated.

Requested Packet Interval (RPI)

When communicating over a network, this is the maximum amount of time between subsequent production of input data.

Routine

A set of logic instructions in a single programming language, such as a ladder diagram. Routines provide executable code for the project in a controller. Each program has a main routine. You can also specify optional routines.

Safety Add-On Instruction

An Add-On Instruction that can use safety application instructions. In addition to the instruction signature used for high-integrity Add-On Instructions, safety Add-On Instructions feature a SIL 3 safety instruction signature for use in safety-related functions.

Safety Application Instructions

Safety Instructions which provide safety-related functionality. They have been certified to SIL 3 for use in safety routines.

Safety Component

Any object, task, program, routine, tag, or module that is marked as a safety-related item.

Safety Instruction Signature

The safety instruction signature is an ID number that identifies the execution characteristics of the safety Add-On Instruction. It is used to verify the integrity of the safety Add-On Instruction during downloads to the controller.

Safety I/O

Safety I/O has most of the attributes of standard I/O except it features mechanisms certified to SIL 3 to ensure data integrity.

Safety Network Number (SNN)

Uniquely identifies a network across all networks in the safety system. The end user is responsible is responsible for assigning a unique number for each safety network or safety subnet within a system. The safety network number makes up part of the Unique Node Identifier (UNID).

Safety Partner

The processor in a dual-processor controller that works with the primary controller to perform safety-related functions.

Safety Program

A safety program has all the attributes of a standard program, except that it can only be scheduled in a safety task. The safety program consists of zero or more safety routines. It cannot contain standard routines or standard tags.

Safety Routine

A safety routine has all the attributes of a standard routine except that it is valid only in a safety program and that it consists of one or more instructions suitable for safety applications (See Appendix A for a list of Safety Application Instructions and standard Logix Instructions that may be used in safety routine logic.)

Safety Tags

A safety tag has all the attributes of a standard tag except that the GuardLogix controller provides mechanisms certified to SIL 3 to ensure the integrity of their associated data. They can be program-scoped or controller-scoped.

Safety Task

A safety task has all the attributes of a standard task except that it is valid only in a GuardLogix controller and that it may schedule only safety programs. Only one safety task can exist in a GuardLogix controller. The safety task must be a periodic/timed task.

Safety Task Period

The period at which the safety task executes.

Safety Task Reaction Time

The sum of the safety task period plus the safety task watchdog. This time represents the worst case delay from any input change presented to the GuardLogix controller until the processed output is available to the producing connection.

Safety Task Signature

A value, calculated by the firmware, that uniquely represents the logic and configuration of the safety system. It is used to verify the integrity of the safety application program during downloads to the controller.

Safety Task Watchdog

The maximum time allowed from the start of safety task execution to its completion. Exceeding the safety task Watchdog triggers a nonrecoverable safety fault.

Standard Component

Any object, task, tag, program, and so on, that is **not** marked as being a safety-related item.

Standard Controller

As used in this document, standard controller refers generically to a ControlLogix controller.

Symbolic Addressing

A method of addressing which provides an ASCII interpretation of the tag name.

System Reaction Time

The worst case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safe state. System Reaction Time includes sensor and activator Reaction Times as well as the Controller Reaction Time.

Task

A scheduling mechanism for executing a program. A task provides scheduling and priority information for a set of one or more programs that execute based on a certain criteria. Once a task is triggered (activated), all of the programs assigned (scheduled) to the task execute in the order in which they are displayed in the controller organizer.

Timeout Multiplier

This value determines the number of messages that may be lost before declaring a connection error.

Valid Connection

Safety connection is open and active, with no errors.

Notes:

Numerics

1734-AENT 16, 17
hardware overview 26
1734-AENTR 16
1756-A10 17
1756-A13 17
1756-A17 17
1756-A4 17
1756-A7 17
1756-CN2
firmware revision 17
hardware overview 26
1756-CN2R
firmware revision 17
1756-DNB
firmware revision 17
hardware overview 26
1756-EN2F
firmware revision 17
1756-EN2T
firmware revision 17
1756-ENBT
firmware revision 17
hardware overview 26
1756-PA72 17
1756-PA75 17
1756-PA75R 17
1756-PB72 17
1756-PB75 17
1756-PB75R 17
1768-CNB 16
hardware overview 26
1768-CNBR
hardware overview 26
1768-ENBT 16
hardware overview 26
1768-PA3 16
1768-PB3 16

A

Add-On Instruction
certify 83
instruction signature 85
safety instruction signature 86
agency certifications 18
application development basics 53
application program
See program

C

CE 18
certifications 18
chassis
catalog numbers 17
hardware overview 24
checklist
GuardLogix controller system 28, 96
program development 99
SIL 3 Inputs 97
SIL 3 outputs 98
CIP safety protocol
definition 103
overview 25
routable system 35
commissioning life cycle 54
communication bridges
hardware overview 26
communication modules
catalog numbers 17
configuration signature 31
connection status 68
CONNECTION_STATUS
data type 67
contact information 22
control and information protocol
Definition 10
control function
specification 55
ControlNet bridge module
hardware overview 26
CSA 18
C-Tick 18
c-UL-us 18

D

DeviceNet Safety
communication overview 27
DeviceNet scanner interface module
hardware overview 26
diagnostic coverage
definition 10

E

EN50156 Compliance 45
EN954-1
CAT 4 9, 13
EtherNet/IP
communication overview 26

EtherNet/IP communication interface module
hardware overview 26
European norm.
definition 10

F

failure
contact information 22
faults
nonrecoverable controller faults 75
nonrecoverable safety faults 75
overriding 75
recoverable 76
FM 18
forcing 62
functional verification tests 14

G

get system value (GSV)
defintion 10
GSV instructions 74

H

hard faults
recovery 75
hardware fault tolerance 101

I

I/O modules
replacement 32-33
IEC 61508
Safety Integrity Level (SIL) 3 certification 9, 13, 86
inhibiting a module 63
installing a controller 23
instruction signature 85
definition 103
instructions
safety 80
safety application 77
ISO 13849-1 9, 13

L

ladder logic safety instructions 80
Logix components
SIL 3-certified 16
Logix system reaction time
calculating 90

M

mapping tags 51
metal form instructions 79

N

nonrecoverable controller faults 75, 103
nonrecoverable safety faults 75, 103
restarting the safety task 75

O

offline edits 64
online
definition 104
online editing 61, 64
output delay time 31
overlap
definition 104
ownership 31

P

partnership
definition 104
peer-to-peer communication 26
pending edits 61
Performance Level
definition 10
period task
definition 104
PLe 9, 13
power supplies 17
hardware overview 24
SIL 3-certified 24
primary controller
definition 104
hardware overview 24
probability of failure on demand (PFD) 19-20
definition 10
probability of failure per hour (PFH) 19-20
definition 10

program
checklist 99
download 61
editing life cycle 65
offline editing 64
online editing 64
upload 61
program compare utility 59
program indentification 56
program verification 57
programming software 13
project
confirmation 58
proof tests 14
see functional verification tests

Q

qualifying standard data 51

R

reaction time
safety task 21
system 21
recoverable faults 76, 104
reliability burden 20
requested packet interval
definition 104
RSLogix 5000 software
changing your application program 63
commissioning life cycle 54
revision 16, 17

S

safe failure fraction 101
safety application instructions 77
definition 105
safety certifications and compliances 18
safety concept
assumptions 53
safety consumed tags
safety network number 38
safety functions
CIP Safety I/O 29
Safety Output 31
safety instruction signature 86
definition 105
Safety Integrity Level (SIL)
compliance distribution and weight 20
function example 16
policy 13-22
Safety Integrity Level (SIL) 3 certification 9, 13, 86
Logix components 16
TÜV Rheinland 14
user responsibilities 14
safety network number 36
definition 105
manual assignment 36
out-of-box modules 38
safety consumed tags 38
safety partner
configuration 24
definition 105
hardware overview 24
location 24
safety program 49
definition 106
safety routine 50
definition 106
safety tags 50
definition 106
valid data types 50
safety task
definition 106
execution 48
overview 47
safety task period 21
definition 106
limitations 48
overview 21
safety task reaction time 21
definition 106
safety task signature
definition 106
deleting 57
generating 57
restricted operations 57
safety task watchdog 21
definition 107
modifying 21
overview 21
setting via RSLogix 5000 21
timeout 48
safety-locking 60
default 60
passwords 60
restricted operations 60
set system variable (SSV) instruction 74

signature history 87
software
changing your application program 63
commissioning life cycle 54
system reaction time 21
calculating 89
definition 107

T

tags
produced/consumed safety data 50
Safety I/O 50
see also safety tags
terminology
used throughout manual 10
timeout multiplier
definition 107

U

UL 18
unique node reference
defined 36

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support/, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/support/.

Installation Assistance

If you experience an anomoly within the first 24 hours of installation, review the information that's contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1756-RM093F-EN-P - January 2010
Supersedes Publication 1756-RM093E-EN-P - July 2008
Copyright © 2010 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.